Next Generation Data Interoperability: It's all About the Metadata

Leslie S. Winters
U.S. Joint Forces Command
J6I, Net-Centric Information Integration Division
1562 Mitscher Ave
Norfolk, VA
leslie.winters@jfcom.mil

Michael M. Gorman
Whitemarsh Information Systems Corporation
2008 Althea Lane
Bowie, MD 20716, USA
mmgorman@wiscorp.com

Dr. Andreas Tolk
Old Dominion University
Engineering Management and Systems Engineering
242B Kaufman Hall
Norfolk, VA 23529
atolk@odu.edu

Keywords:

Interoperability, Joint Command and Control, Net-Centric Data Strategy, Data Modeling, Data Standards, Data Sharing, Metadata, Metadata Registry, Community of Interest, Modeling and Simulation

ABSTRACT*: Data interoperability has been an objective of the DoD for as long as automated systems have been in existence, particularly in the area of Command and Control (C2). Long time DoD efforts to achieve data interoperability through data element standardization were not successful, and these efforts have been superceded by the 2003 DoD Net-Centric Data Strategy. This approach seeks to capitalize on successes in the commercial IT sector through the use of web-based technologies and the concept of Service Oriented Architecture (SOA). The key to this approach is the metadata that describes the data and services being shared. Several DoD Communities of Interest (COI) are now producing and publishing metadata artifacts in the DoD Metadata Registry. Programs of Record participating in these COIs are also beginning to use these artifacts to expose their data via web services in various experiments and exercises.*

While the current approach will ultimately make data visible and accessible to the enterprise, the data is currently only truly understandable and interoperable within the COI. Data understanding and interoperability across COIs remains a manual, ad-hoc process, and "on-the fly" machine-to-machine data interoperability and composition of services is not supported. In order to improve current efforts to implement the DoD Net-Centric Data Strategy and move toward the level of interoperability that is required for dynamic data exchange and composition of services, it is necessary to rethink how metadata is defined, organized, and managed.

This paper proposes an approach for "next-generation" implementation of the DoD Net-Centric Data Strategy that includes a comprehensive metadata repository exposing all the details of the data's definition and the mapping of this data through the systems that generate the standardized transactions. Specifically, an ISO/IEC 11179-3 compliant Metadata Registry with COI efforts directed toward producing metadata products consistent with this standard is endorsed, with the metadata registry artifacts integrated into a distributed and federated metadata repository environment. Application to Joint C2 capabilities and implications for M&S, a key aspect of C2, are also discussed.

1 Background

Joint Command and Control (C2) interoperability has been an issue for as long as automated C2 systems have been in existence, and well prior to that whenever armed forces with heterogeneous languages, organizations, and tactics have allied themselves against a common adversary. A 1987 Government Accountability Office (GAO) report [1] cites examples of Joint C2 interoperability concerns going back to the Vietnam era and reports that little progress had been made in the 20 years hence, despite publication of the DoDD 4630.5 Interoperability policy in 1967 [2] and the formation of the Joint Tactical Command, Control, and Communications (C3) Agency.

Today, nearly another 20 years later, Joint C2 interoperability is still challenging the DoD as documented by Starr [3] and many others. With the advent of Net-Centric Operations and Warfare to satisfy the need for Information and Decision Superiority [4], there is now an unprecedented reliance on rapidly changing IT technology, leading to an even more complex technical problem space. In addition, the same management impediments cited in the 1987 GAO report and elsewhere still exist:

- DOD's decentralized management structure
- Lack of clearly defined joint requirements for interoperability
- The absence of an effective central enforcement authority to make the necessary interoperability decisions.

This continued challenge of Joint C2 interoperability has been a key topic during several recent Joint forums including the C2 Senior Warfighter Forum in February 2006 and United States Joint Forces Command (USJFCOM) Component Commanders Meetings in March and May 2006. It was also a large factor leading to the creation of a Command and Control Integration Board and a Joint C2 Capability Area, with USJFCOM designated the Command and Control Capability Area Portfolio Manager [32, 33].

Modeling and Simulation (M&S) to C2 interoperability is a related challenge with additional considerations that have arisen with the use of M&S to support Joint C2 training, experimentation, analysis, and mission rehearsal. While M&S has traditionally been regarded as being distinct from C2, M&S capabilities are becoming increasingly important to support operational C2 functions such as Planning and Course of Action Analysis. Thus, the line between M&S and C2 is becoming increasingly blurred.

An encouraging development supporting joint interoperability for both M&S and C2 is the advent of the Global Information Grid (GIG) [5], the concept of Service Oriented Architecture [6], and the DoD Net-Centric Data Strategy [7]. Capitalizing on successes in the commercial sector, the DoD is transforming the way that IT capabilities are constructed and interoperate using internet-based methods, technologies, and standards. The same technology that enables e-Bay, Google Earth, and e-commerce will allow the DoD to more readily share data and mix-and-match functions (services) to create needed capabilities. The main idea is to publish descriptions of composable services that provide a required functionality. In case of need, a user or another service/system can discover these services and establish the necessary information exchange between his system and the service provider via web-technology.

A key concept in this new approach is metadata, or simplistically, "data about data." Metadata describes the meaning and structure of data, where to find it, and how to access it through web services. Advanced metadata engineering expands the definition of metadata to include all the process, system, mission, function, and transformation specifications that provide data its full semantic context. Additionally, such expansions allow the mapping between systems and databases in support of increased levels of interoperability.

While this new approach to interoperability holds much promise for the DoD, the transformation is in its infancy and there are many practical details of implementation that must be addressed to enable further progress. A particular area needing attention is metadata definition, organization, and management.

In this paper, we summarize the main results of an independent study to identify the shortcomings of recent DoD data activities and make recommendations for current and future activities. We start with a general overview of the problem domain in section 2. In section 3, we discuss past and current DoD approaches to data interoperability. Section 4 describes the current DoD approach to metadata and registries. Section 5 proposes a "next generation" solution as recommended by the authors, focused on improvements to the DoD Metadata Registry (MDR). Specifically, an ISO/IEC 11179-3 compliant Metadata Registry [8] is proposed such that its metadata specifications can be integrated with the contents of the MDR and enable the integration of all MDR metadata. Finally, in section 6 we summarize the results and give recommendations for SISO.

2 Levels of Interoperability

Before discussing specific DoD data and metadata interoperability approaches and challenges, a general view of the problem domain and objective is needed. It is helpful to begin by defining and categorizing interoperability. The DoD definition of interoperability is:

"… the ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces and to use the services so exchanged to enable them to operate effectively together without altering or degrading the information exchanged." [9]

For the purposes of this paper, there are three useful perspectives on interoperability:

- the Organizational Perspective,
- the IT Systems Perspective, and
- the Data Perspective.

2.1 Organizational Perspective

An organizational perspective on interoperability is described by Clark and Jones as the *Organizational Interoperability Maturity Model (OIMM)* [10]. This model is not focused on information technology-based interoperability, but rather on the human aspects of interoperability such as common goals, common approaches, shared understanding, established mechanisms for interaction, etc. Like the more familiar Levels of Information Systems Interoperability (LISI) model described in the following section [11], the OIMM consists of 5 levels, each representing a greater level of interoperability than the previous level:

- **Level 0 (independent):**
  Organizations that do not share common goals or purposes but may be required to interact on rare occasions
- **Level 1 (ad hoc):**
  Organizations that have some overarching shared goals but interaction is minimal, there are no formal mechanisms for interacting, and organizational aspirations take precedence over shared goals.
- **Level 2 (collaborative):**
  Frameworks are in place to support interoperability and there are shared goals, but organizations are distinct.
- **Level 3 (combined):**
  Organizations interoperate habitually with shared understanding, value systems, and goals, but there are still residual attachments to a home organization.
- **Level 4 (unified):**
  The organization is interoperating continually with common value systems, goals, command structure/style, and knowledge.

The nirvana of Joint C2 from the operational perspective is to act as a Level 4, unified force. This is characterized by an interdependent, collaborative, learning, adaptive, and coherently Joint Force as shown in Figure 1, a common slide used by USJFCOM to depict transformation to an effective Joint force.

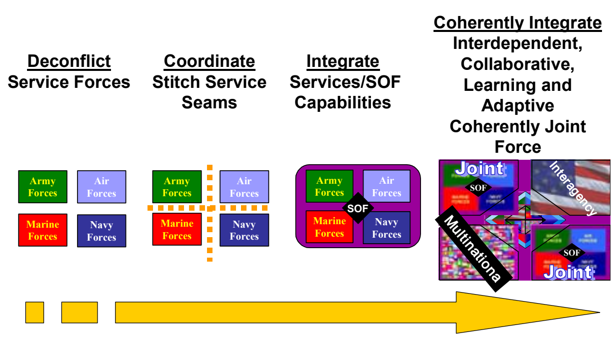

Figure 1: Transformation to a Joint Force

2.2 IT Systems Perspective

From an IT systems perspective, interoperability is defined by how systems are physically interconnected. This is the most familiar perspective on interoperability and is traditionally represented by the C4ISR Architectures Working Group's *Levels of IT Systems Interoperability (LISI)* model [11]. The 5 levels of the LISI model are as follows:

- **Level 0 (isolated):**
  Systems need to exchange data but cannot physically interoperate. Information sharing is manual
- **Level 1 (connected):**
  Systems are connected by peer-to-peer connections. Simple (homogeneous) data products can be exchanged.
- **Level 2 (distributed/functional):**
  Systems are connected to multiple systems on a LAN and can exchange complex (heterogeneous) data for a specific function.
- **Level 3 (integrated/domain):**
  Systems and applications are interconnected, with shared applications and data within a specific functional domain.
- **Level 4 (enterprise)**:
  Enterprise-wide shared applications and data.

While the organizational interoperability levels of the OIMM are not directly linked to the systems interoperability levels of the LISI model, they are closely related in that higher levels of systems interoperability support and promote higher levels of organizational interoperability. Conversely, lower levels of systems interoperability hinder organizational interoperability, particularly when an organization depends on IT to perform its core mission. A loose relationship between the LISI and the OIMM is shown in Figure 2.

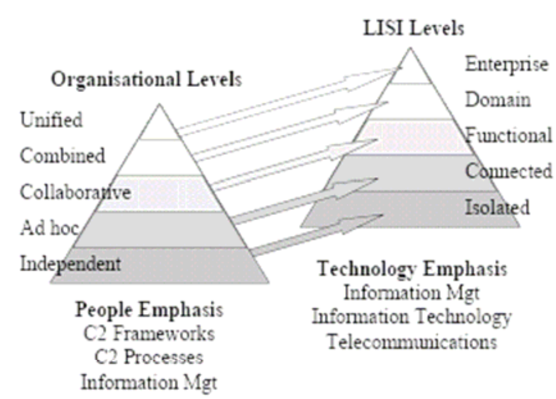

Figure 2: Relationship between LISI and OIMM [10]

2.3 Data Perspective

What is lacking from the previous views of interoperability is the data that is exchanged between the systems and organizations. Is the right data exchanged? Can the systems readily receive, interpret, and process it into useable formats? Does the data meet the organizational information requirements, to include requirements for timeliness, accuracy, and security? The information, data, and metadata flowing between the systems and organizations are the real currency of interoperability. This requires a third perspective on interoperability: the data perspective.

While the LISI describes the physical connections between systems and the type of data that is shared, it does not describe how the data is interpreted or understood by the interoperating systems or organizations in order to share data in a meaningful way. At the highest levels of organizational interoperability, this shared understanding of the data goes beyond the syntax or semantics of the data. It requires an understanding of the context of the data and the very concepts that the data represents. In 2003 Tolk and Muguira proposed a 5-tiered *Levels of Conceptual Interoperability Model (LCIM)* that describes interoperability from the data perspective [12]. This model was further refined in [13] to the 7-layer model shown in Figure 3.

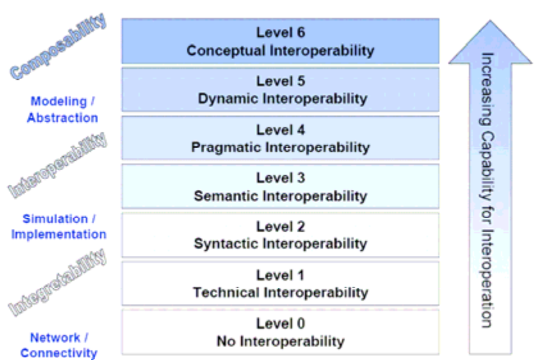

Figure 3: Levels of Conceptual Interoperability Model (LCIM)[13]

The 7 layers of the LCIM are as follows:

- **Level 0 (No Interoperability)**:
  Stand-alone systems- no data is shared.
- **Level 1 (Technical Interoperability):**
  A communication infrastructure is established, underlying networks and communication protocols are unambiguously defined.
- **Level 2 (Syntactic Interoperability):**
  A common protocol to structure the data is used; the format of the information exchange is unambiguously defined.
- **Level 3 (Semantic Interoperability):**
  The meaning of the data is shared through the use of a common reference model and the content of the information exchange requests are unambiguously defined.
- **Level 4 (Pragmatic Interoperability):**
  The meaning of the data and the context of its use are "understood" by the participating systems, and the context in which it is exchanged is unambiguously defined.
- **Level 5 (Dynamic Interoperability):**
  Systems are able to comprehend the state changes that occur in each other system's assumptions and constraints over time; thus, the effect of the information exchange is unambiguously defined. (Particularly important to M&S applications).
- **Level 6 (Conceptual Interoperability):**
  The conceptual models underlying the data in each system are aligned. This requires that conceptual models be documented as "fully specified but implementation independent models" as suggested in Davis and Anderson [14], enabling their interpretation and evaluation by other engineers.

Furthermore, LCIM utilizes the three categories introduced by Page et al. in [15]:

- **Integratability** addresses the physical/ technical realms of connections between systems, which include hardware and firmware, protocols, etc.
- **Interoperability** addresses the software- and implementation details of interoperations; this includes exchange of data elements based on a common data interpretation.
- **Composability** addresses the alignment of issues on the modeling level. The underlying models are purposeful abstractions of reality used for the conceptualization being implemented by the resulting simulation systems.

The LCIM adds a new dimension to the understanding of interoperability that bridges the gap between systems interoperability and organizational interoperability. This is because it bridges the gap between raw data that is exchanged between systems and the higher human understanding of the concepts that data represents in a given context. A truly unified organization has common value systems, goals, command structure/style, and knowledge per the OIMM. This is akin to conceptual interoperability of data per the LCIM on an enterprise-wide scale per the LISI. The relationship between the LISI, LCIM, and OIMM models is shown in Figure 4. The conclusion one may draw is that enterprise level systems interoperability with conceptual interoperability of data can support and promote unified interoperability of an organization. This is because high levels of interoperability from a systems and data perspective will lead to the shared understanding that is required from the organizational perspective in an organization that is dependent on IT.

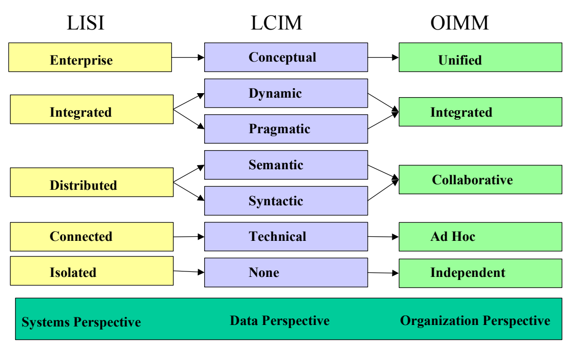

Figure 4: LISI, LCIM, and OIMM Relationships

With regard to Joint C2, Unified Interoperability for a Joint organization can be greatly enhanced by enterprise-wide conceptual data interoperability that allows for the free exchange and fusion of data between many diverse sources (to include M&S) and elements of the organization to create a common, consistent, and accurate representation of the battlespace. At its highest level, conceptual interoperability of data allows for "on-the fly" composition of web-services and data to create needed capabilities. This is referred to as the "dynamic web" by Tolk [16].

3 DoD Approaches to Data Interoperability

As evident from the previous section, syntactic and semantic data interoperability is necessary (but not sufficient) to achieve meaningful levels of interoperability between systems and organizations that strive to collaborate toward a common goal. In order to achieve these levels of data interoperability, systems and organizations must be able to represent and share the meaning of a data in an unambiguous manner. This requires unambiguous data definitions and metadata capturing this information.

DoD recognizes the need for syntactic and semantic data interoperability as well. In 1964, the DoD issued its first policy regarding data interoperability in the form of DoD Directive 5000.11, "Data Elements, and Data Codes Standardization Program" [17]. This policy was reissued in 1991 as DoDD 8320.1, "DoD Data Administration" [18]. Both of these policies focused on DoD-wide data element standardization, the latter in the larger context of sound data administration practices.

The most recent DoD policy related to data interoperability is DoDD 8320.2, "Data Sharing in a Net-Centric Department of Defense" [19], which directs implementation of the 2003 DoD Net-Centric Data Strategy [7]. This approach abandons attempts at DoD-wide data element standardization in favor of common data vocabularies, taxonomies, and XML schemas established within functional domains, called Communities of Interest.

The following sections describe the latter two of these approaches, to include shortcomings and areas for improvement.

3.1 DoDD 8320.1: Data Administration

The stated objectives of DoDD 8320.1 were to:

- Support DoD operations and decision-making with data that meets the need in terms of availability, accuracy, timeliness, and quality; and
- Structure Information Systems in ways that encourage horizontal, as well as vertical, sharing of data in the Department of Defense, and with other Government Agencies, private sector organizations, and allied nations, consistent with national security and privacy requirements.

Like the previous policy, DoDD 8320.1 centered on standardizing data elements across the DoD. However, 8320.1 did so in the larger context of data administration procedures that improve the way an organization uses data by defining data structuring rules and standards and planning for the efficient use of data. A centerpiece of DoDD 8320.1 was the DoD Information Resource Dictionary System (DoD IRDS), implemented as the Defense Data Repository System (DDRS). This was the repository for information on the standard defense data elements, their definitions, allowable values, etc. In terms of the previous section and Figure 4, DoDD 8320.1 was attempting to achieve Enterprise-wide semantic interoperability to facilitate collaborative interoperability between organizations that were connected in a distributed manner.

While the goals of the policy were admirable, practically the 8320.1 approach never succeeded. A common misconception about the failure of 8320.1 is that it was not possible to reach the consensus required to standardize data elements across the DoD. However, the failure of the policy was much more fundamental. According to a 1994 GAO report [21], the failure was that *DoD had not properly identified its business requirements for data before proceeding to standardize data elements.* In other words, the context of the use of data as requested by the level of pragmatic interoperability in the LCIM was not defined. Furthermore, guidance on developing, validating, integrating, and approving the data models from which data standards are derived was never issued. This, coupled with shortcomings of the DDRS and the associated data element standardization process, resulted in a vast collection of questionable information about DoD data elements that were not at all standard.

An internal MITRE study[1], also in 1994, came to similar conclusions regarding the effectiveness of DoDD 8320.1 and its associated implementation procedures. This study identified the following shortcomings:

- A fundamentally flawed data standardization model that was focused exclusively on data elements with an intractable data element naming convention
- A definition of "data element" such that it was literally a column within a database table. Thus, the workload was constantly expanding as the quantity of databases, tables, and columns constantly expanded.
- No accommodation for enterprise wide data architectures, thus related data elements were "standardized" separately
- No accounting for multiple implementation approaches that represent the same data element differently
- A central standardization and maintenance authority that could not realistically meet its responsibilities across the DoD.

All of these shortcomings, coupled with the new demands of net-centricity and advances in the commercial IT sector, ultimately led to a new DoD approach to data.

3.2 DoD Directive 8320.2: Data Sharing in a Net-Centric Department of Defense

The current DoD approach to data interoperability is embodied in the May, 2003 "DoD Net-Centric Data Strategy" [7], DoDD 8320.2, "Data Sharing in A Net-Centric Department of Defense" [19], and DoDD 8320.2-G, "Guidance for Implementing Net-Centric Data Sharing" [20]. The Net-Centric Data Strategy (NCDS) is based on industry best practices that were gleaned from Internet approaches to sharing data. Key features of the NCDS include:

- The goals of the NCDS are larger than data interoperability and include making data visible, accessible, understandable, trusted and secure.
- The NCDS is based on the Service Oriented Architecture (SOA) foundation of the GIG and relies on industry standards such as XML, WSDL, SOAP, BPEL, etc. to expose and share data via web services.
- Enterprise-wide data element standardization, as defined and required in 8320.1, is no longer an objective and there is no central data element standardization authority.
- Data "standardization" efforts focus on vocabulary and XML schemas and are undertaken by joint (ideally) Communities of Interest (COIs); cross-Service groups of data producers and consumers that habitually share information "and must therefore have a common vocabulary."
- The DoD Metadata Registry replaces the DDRS as the central repository of data/metadata artifacts, including vocabularies, taxonomies, XML schema definitions, and the 8320.1 data elements.

The 8320.2 approach has several advantages over earlier DoD approaches to data. A key advantage of the 8320.2 approach is that the use of the SOA construct, XML technology, web-services, and discovery metadata effectively separates data from applications and makes it visible and accessible across the enterprise using common standards. This is an important step toward large-scale interoperability that leverages commercial successes and opens the door for sharing data with the much-heralded "unanticipated user," as well as interoperating with commercial software. This concept is illustrated in Figure 5, a slide commonly used in ASD(NII)/DoD CIO data strategy briefings.

Another advantage of the 8320.2 approach is that it relies on COIs to develop common data products and the associated metadata. This eliminates the bottleneck at the approval authority that was an issue in the 8320.1 era and makes key stakeholders (e.g. Programs of Record and users) part of a Joint solution through their participation in the COIs.

A third advantage is that the scope of the data products and the content of the DoD Metadata Registry is larger than just data elements and includes vocabulary, taxonomy, and XML schema descriptions. This gives a broader context to the data elements that was missing in the 8320.1 approach.

[1] A technical report documenting the results of this study was never published, but one of the authors participated in the study.

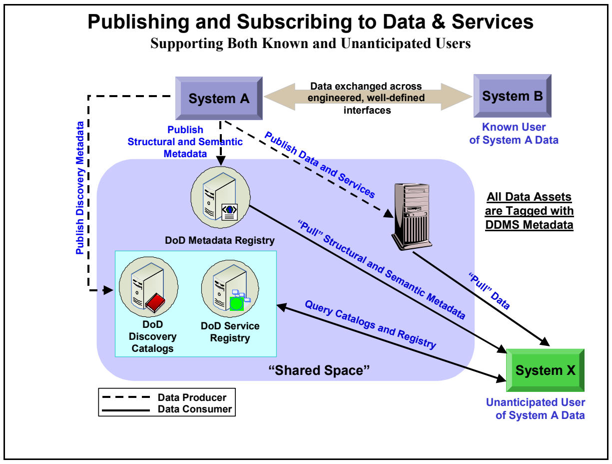

Figure 5: DoD Net-Centric Data Strategy Concept of Operations

The ultimate objective of the NCDS is to enable the exchange of unambiguous descriptions of data and services (metadata) that allows for the discovery and reuse of data and services on the GIG. In terms of the previous section and Figure 4, the 8320.2 approach is seeking semantic data interoperability within a functional domain (COI) and between functional domains where needed via translations. The IT infrastructure is enterprise wide (the GIG), and the level of organizational interoperability targeted would appear to be collaboration within a COI.

3.3 Current Status and Implementation Activities

Despite initial (and in some cases lingering) resistance of many DoD stakeholders, the DoD is making tangible progress implementing the Net-Centric Data Strategy. The Services are developing Service-specific implementation policy and processes, Mission Area leads are developing governance and management mechanisms [22, 23], and individual Programs of Record such as the Army's Future Combat System and DISA's Net-Enabled Command Capability, are increasingly working with COIs to adopt their data products. At present there are over 50 registered COIs [24], with approximately 10 considered effective by the authors in that they have appropriate stakeholder membership, are producing the required data products to populate the DoD Metadata Registry, and are beginning to effect change in programs of record by making their data visible and accessible and understandable via XML tagging and web-services. In addition, many COI-like activities are taking place within organizations such as the GEOINT Working Group, and individual programs of record such as the Army Battle Command System and the Defense Common Ground Station are taking actions to become "net-centric" (e.g. implementing web-services and standards) outside of a formal COI.

While much progress has been made, there is room for improvement and several areas warrant attention to fully realize the advantages of the 8320.2 approach. Deficiencies noted in the draft ASD(NII)/DoD CIO report on Data Strategy Implementation [34] include:

- There is no systematic process to measure implementation of the NCDS, determine value to the operator, or assess unsatisfied data needs.
- Many COIs lack adequate cross-Component participation and lack a mechanism for informing portfolio management processes.
- DoD Components require additional technical guidance to implement visibility and accessibility goals.
- The Joint Capabilities Integration and Development System, the Defense Acquisition System, and the Programming, Budgeting and Execution process do not provide needed models for identifying, acquiring, and resourcing net-centric information sharing capabilities.

Additional shortcomings observed by the authors and discussed in various DoD Data Strategy implementation forums[2] include:

- No methodical identification or prioritization of COIs according to DoD data sharing needs.
- Continuing lack of buy-in and/or understanding of the data strategy coupled with lack of resources to incentivize formation of and participation in COIs.
- Limited management and technical provisions for enabling cross-COI data interoperability.
- No specified baseline data products for COIs or guidance on how to produce them, leading to potentially incompatible products and high variations between COIs.

Many of these shortcomings are the required growing pains of implementing the Information Transformation represented by the GIG, Service Oriented Architecture, and the DoD Net-Centric Data Strategy. Thus, identification of them here should not be construed as an indictment of the various agencies involved. In fact, many of these deficiencies are being addressed by ASD(NII)/DoD CIO, Mission Area Leads, DISA,

[2] Example DoD Data Strategy forums include a USJFCOM-hosted COCOM Data Strategy Implementation Workshop, WMA COI governance meetings, GIG Information Sharing Sessions, USJFCOM Component Commander's meetings, the COI Forum, and meetings of the Time Sensitive Targeting and Blue Force Tracking COIs.

USJFCOM, and others as the implementation process evolves.

Two promising developments for the Joint Warfighter and Joint C2 interoperability are the creation of a Warfighter Mission Area COI governance body and the effort by USJFCOM to integrate the C2-related COIs into its Portfolio Management processes for the C2 Capability Area. The WMA COI governance body is chaired by the Joint Staff (JS) J6 and includes membership from all of the Services, COCOMs, DISA, ASD(NII)/DoD CIO, the JS IT Portfolio Managers, and representatives from the 3 remaining GIG IT Mission Areas. Its purpose is to collectively manage the activities of the WMA COIs, resolve cross-COI issues, and link the activities of the WMA COIs with the IT Portfolio Management process. This body has been functioning since December 2005 and is becoming a valuable forum for maintaining awareness of COIs and NCDS developments, identifying and resolving issues within the WMA and between the WMA and other Mission Areas, and generally advancing NCDS implementation progress through mutual support of the organizations involved.

Within the C2 arena, the designation of USJFCOM as the C2 Capability Portfolio Manager (C2 CPM) and the intent to integrate the activities of the C2-related COIs into the C2 CPM processes bodes well for C2 data interoperability and implementation of the NCDS within C2 capabilities. While this effort is just now forming, the intent is to actively manage the C2-related COIs as a group and synchronize their activities with the objectives of the C2 CPM. This will ensure that C2-related COIs are focused on C2 CPM data interoperability priorities, enable consistent implementation of the NCDS across C2 COIs, facilitate interoperability between C2-related COIs, and allow for efficiencies in operating C2 COIs.

These two efforts are very important and will provide mechanisms to address several of the noted shortcomings with NCDS implementation, many of which are management-related. However, one notable area still requiring particular attention as implementation of the Net-Centric Data Strategy evolves is the definition, organization, and management of the various types of metadata in the DoD Metadata Registry. This topic is discussed in the following section.

4 DoD Metadata Registry

As the concepts of Net-Centric Operations and Warfare, the GIG, the Net-Centric Data Strategy, and even Service Oriented Architecture have become more and more pervasive at the highest ranks, a common mantra heard in many executive level meetings is "It's all about the data". (Repeat multiple times.) While it is great progress and laudable that this level of attention is being afforded to data, in reality the mantra should be "It's all about the metadata." Structural, semantic, and discovery metadata is the cornerstone to making data visible, accessible, understandable, trusted, secure, and interoperable in accordance with the goals of the Net-Centric Data Strategy. The DoD Metadata Registry and Clearinghouse (MDR) is a key element of the Net-Centric Data Strategy, which describes the MDR as *"... a one stop shop for developer data needs… a comprehensive source for supporting design, development, and execution of processes (e.g. business logic) in a Net-Centric, services-based data environment."* Through the MDR, DoD software developers can access and reuse XML data and metadata components, Common Operational Environment (COE) database segments, and reference data tables and related metadata information.

The Metadata Registry consists of four key galleries: XML, Taxonomy, Reference Data Set, and Data Element, described as follows: [25]

- **XML Gallery:** XML information resources such as submission packages, elements, attributes, and schemas that have been registered by DoD software developers or COIs.
- **Taxonomy Gallery:** XML-based taxonomy files that describe one or more nodes in a hierarchical classification of items, and their relationships to other nodes.
- **Reference Data Set Gallery:** Collections of related data that represent a defined entity within a community of interest. Examples of reference data sets include country codes, U.S. state codes, and marital status codes.
- **Data Element Gallery:** Manages relationships that may exist between data elements within the Metadata Registry. Developers using data elements provided in the submission package's manifest file define most relationships. Other relationships are defined automatically during the processing of submitted registry documents. The Data Element Gallery provides guidance in the generation and use of XML among DoD communities of interest and is the authoritative source for registered XML data and metadata components.

The MDR is currently implemented via separate[3] Unclassified, Secret, and Top Secret instances and includes runtime support via web services and electronic business XML (ebXML) capabilities. As of 17 May 2006, the MDR contained over 130,000 data artifacts and over 7,000 registered users from the DoD, Intelligence

[3] MDR content from lower classified instances is replicated in higher classified instances.

Community, Department of Homeland Security, and the National Aeronautics and Space Agency. [31]

While the MDR is becoming more and more viable, a number of shortcomings still persist. An OCT 2005 MITRE technical report [26] recommended several actions to address some of the most critical shortfalls at the time:

- Provide distinct support for COIs and Namespaces to emphasize and separate the important role of COIs in implementing the NCDS.
- Integrate NCES mediation services with MDR capabilities and use context ontologies to support mediation between data representations.[4]
- Provide better user support, to include improved search/discovery capabilities facilitated by augmented metadata, guidance on best practices for creating quality content, and a streamlined registration, update, and versioning process.
- Cross-link the MDR to related information sources such as the COI directory, the Service Registry, and various data catalogs[5].
- Improve and expand the machine-usable interface to the MDR.

DISA is aware of these shortcomings and has been making steady improvements to the MDR as funding levels allow. For example, version 5.2 of the MDR addresses some of the shortcomings in user support by providing updates and fixes, an improved Manifest Generator, additional tools for Namespace Managers, and updated user's manuals. In addition, NCES mediation services are reportedly being integrated with the MDR to support data mediation via XSLT[6], and DISA releases new features in the MDR quarterly to coincide with the Metadata Working Group meetings. Suggestions for MDR improvements can be submitted anytime through the MDR web page, and DISA prioritizes and addresses these requirements as part of its configuration management process.

Despite these ongoing improvements, a major drawback of the MDR continues to be that there is little integration of metadata artifacts within or between the galleries, and no integration between the MDR and related data stores such as the DDMS, the COI registry, and the DISR. In addition, there are few management controls in place to manage the collections, potentially leading to redundant, outdated, and otherwise inaccurate information that is difficult to search and understand. While the recent addition of a high-level DoD Core Taxonomy and a capability by which users can identify relationships between data elements will help to some extent, what is really needed is an overarching metadata model. Without this, the MDR will continue to become an eclectic collection of various products from COIs, Namespace Managers, Programs of Record, and other sources. As the collection grows, this will not adequately support reuse or interoperability of data. In terms of Figure 4, it is not clear that the current MDR supports even syntactic interoperability between any users other than those who are directly involved with developing specific metadata artifacts for the MDR, e.g. through participation in a COI.

5 Next Generation Data Interoperability

Next generation data interoperability must get beyond the current shortcomings of data strategy implementation efforts to better support anticipated and unanticipated users and developers who want to discover and access data and services and perhaps compose new, interoperable capabilities. Ultimately, next generation data interoperability should strive to support dynamic discovery and access of data as well as dynamic composition of services. Both of the above require a comprehensive metadata repository that exposes all the details of the data's definition and the mapping of standardized data through the systems that generate the standardized transactions. The ISO/IEC 11179 standard for metadata registries supports such an approach.

5.1 ISO/IEC 11179

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) form the specialized system for worldwide standardization. ISO/IEC 11179, Information Technology – Metadata Registries (MDR), primarily addresses the semantics of data element metadata, the representation of data element metadata, and the registration of descriptions of that data element metadata in a metadata registry. The standard was developed in the late 1990's and has undergone several updates to maintain currency, some as recently as 2005. The purpose of the standard is to promote the following:

- Standard description of data element metadata including the semantic supports for data elements, which are data element concepts, concepts, conceptual value domains, value domains, the mapping among value domains, and data element classifications.

---

[4] Paper [27] introduced ideas for data engineering and data mediation and showed how to implement this.

[5] Important information sources suitable for linking but not mentioned in the report include the Defense Architecture Repository System and the Defense IT Standards Repository.

[6] This idea has been promoted via NCES briefings, but it is not clear when real-time mediation via XSLT registered in the MDR will be available for use.

- Common understanding of data across and between organizations
- Re-use and standardization of data element metadata
- Harmonization and standardization of data element metadata within and across organizations
- Management and re-use of the components of data element metadata

ISO/IEC 11179 has six parts, each addressing a different aspect of the purposes above.

- Part 1 – Framework:
  Overview of the standard and basic concepts
- Part 2 – Classification:
  How to manage a classification scheme in an MDR
- Part 3 – Registry Metamodel and Basic Attributes: Provides the basic conceptual model, attributes, and relationships for an MDR
- Part 4 – Formulation of Data Definitions:
  Rules and guidelines for defining data elements and their components
- Part 5 – Naming and Identification Principles:
  How to form naming conventions for data elements and their components
- Part 6 – Registration:
  Roles and requirements for the metadata registration

Several agencies worldwide have successfully implemented all or parts of the ISO/IEC 11179 standard. US government implementations include the Department of Justice Global Justice XML Data Model, the Environmental Protection Agency Environmental Data Registry, the Census Bureau FactFinder, the National Cancer Institute Cancer Data Standards Repository, and the US Health Information Knowledgebase. In addition, there are vendor tools available that claim compliance with the ISO/IEC 11179 standard, to include the Oracle Enterprise Metadata Manager and Data Foundations Metadata Registry. (Note that there are no independent agencies established to verify ISO/IEC 11179 compliance.)

5.1.1 Part 3, Registry Metamodel and Basic Attributes

While all parts of the ISO/IEC 11179 registry standard warrant review and consideration, the power of the standard in terms of promoting data interoperability is primarily manifest in Part 3, Registry Metamodel and Basic Attributes. This section specifies a conceptual model for an MDR and its contents. As shown in Figure 6, there are 10 different classes of administered components specified in ISO/IEC 11179-3, and additional components may be defined as extensions to the standard.

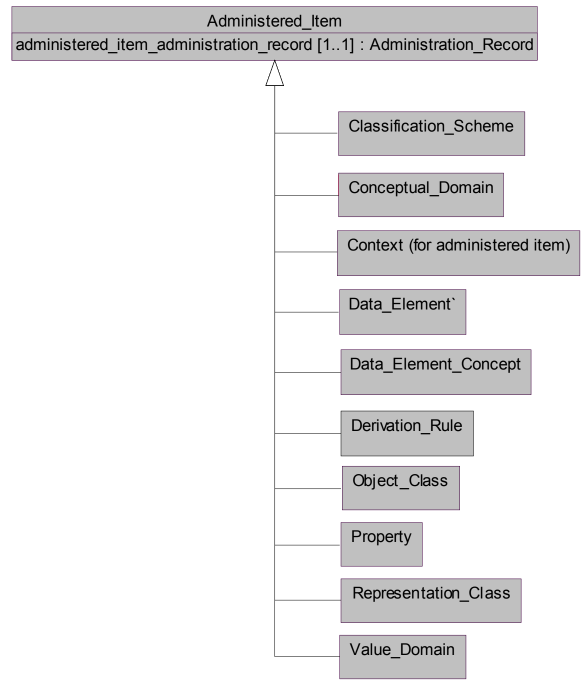

Figure 6: ISO/IEC 11179-3 Administered Items

Key definitions[7] within 11179-3 include:

Object Class: *A set of ideas, abstractions, or things in the real world that are identified with explicit boundaries and meaning and whose behaviors follow the same rules*

Conceptual Domain: *A set of valid value meanings, defined as the meaning or semantic content of a data value.*

Value Domain: *A set of permissible data values*

Data Element Concept: *A concept that can be represented in the form of a data element, described independently of any particular representation.*

Data Element: *A unit of data for which the definition, identification, representation, and permissible values are specified by mans of a set of attributes.*

Fundamentally, the two key components of 11179-3 are *Object Classes*[8] that support the identification and

---

[7] Some definitions are composite definitions created by the authors when the definition of one word included a word that was defined separately in the standard.

[8] A close reading of the standard shows that the intent for *object classes* is that they represent the concepts about which data elements are to be ultimately constructed. Object class

definition of the concepts about which data elements are ultimately specified, and *Conceptual Domains* that broadly identify and describe the concepts behind the value domains that are to be employed.

When Object Classes and Conceptual Domains are brought together, they form *Data Element Concepts*. When Data Element Concepts and Value Domains are brought together they form *Data Elements*. Data Elements then are semantic representations that can be used to build columns within tables, fields within files, data elements within vocabularies and schemas, etc.

Once Data Elements are built they can be set within various *Data Element Classifications,* such as taxonomies and ontologies. A high level metamodel depicting these relationships is shown in Figure 7. This version appears in the standard documentation and has been used in innumerable presentations, although it only captures four of the five main components of metadata registries as defined above.

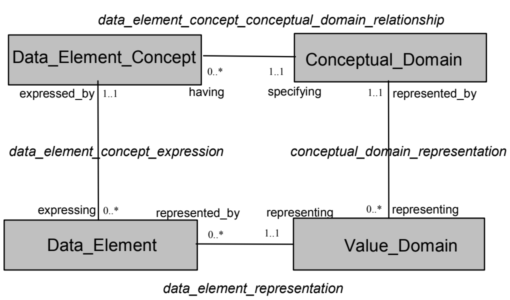

Figure 7:ISO/IEC 11179-3 High Level Metamodel

A better way to visualize these main components is as shown in Figure 8. The Object Class represents a model resulting from the purposeful abstraction of reality. Data element concepts and value domains define data elements. The value domains and data element concepts are both part of the conceptual domain, which captures the application domain of which the object class is part.

here is not to mean entity or table, but a term describing something in the real world (or not) the application is representing. The literature on ontological spectrum refers to this as concepts.

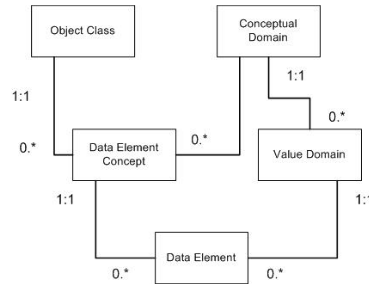

Figure 8: High-level View (proposed)

Figure 9 shows an even more detailed representation by breaking the associations into higher detailed relations.

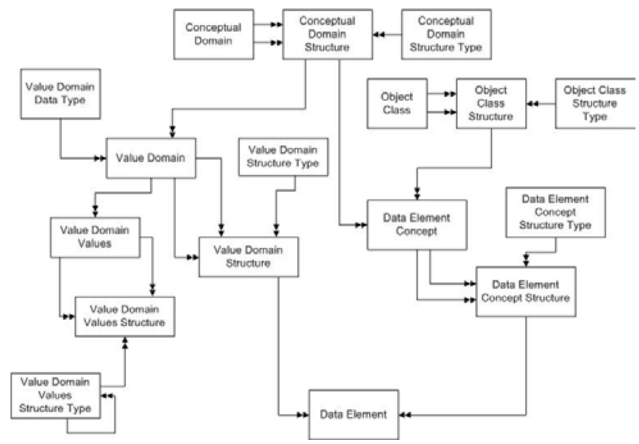

Figure 9:Detailed Representation

A unique characteristic of the ISO/IEC11179-3 metadata model is that Object Classes, Conceptual Domains, Data Element Concepts, Value Domains, and Data Element Classifications are each able to support an internal network structure so as to ultimately support truly sophisticated data elements.

These 11179-3 metamodels support data interoperability because, unlike the DoDD 8320.1 "data element" standardization effort, ISO/IEC 11179-3 does not operate at the database table column level. Rather it operates at a higher level of generalization so that there can be a "define once" use many times approach. With the ISO 11179-3 Data Element definition approach, the names of actual columns or fields in a physical database or in an XML schema can be different from the ISO 11179-3 data elements[9], but the relationship between the physical database or XML schema and the concepts represented is not lost. This facilitates mapping between two or more data elements that represent the same concept and paves the way for machine-to-machine dynamic interoperability. This type of mapping is not supported by the current

[9] Within reasonable restrictions, this is true for data types and value domains as well.

MDR because data elements are not mapped to concepts that are themselves part of the MDR. Rather, relationships between data elements must be explicitly defined and represented on a pair-wise basis via the MDR feature whereby a user can specify when two data elements appear to be the same, or via an XSLT between two XSDs. In either case, the current approach is a manual process that does not readily support unanticipated users or machine-to-machine dynamic interoperability.

In terms of the LCIM of section 2, using the ISO 11179-3 data element metadata approach elevates data interoperability to the semantic level (3) and possibly the pragmatic level (4) if enough metadata about the context of usage is also represented. Higher levels of interoperability are possible if the data element is part of a sufficiently rich conceptual model that is implemented in the registry. However, creation of the appropriate conceptual model is a difficult problem that is not solved by 11179-3.

5.1.2 Applicability of ISO/IEC Parts 2, 4, 5, and 6

Although it is only necessary to implement Part 3 of the ISO/IEC 11179 standard to facilitate data interoperability as described in the previous section, all parts of the standard are worthy of consideration for improving the DoD metadata development and management process.

Parts 4 and 5 of the standard address data element definitions and data element naming conventions. This guidance could prove useful to COIs as they develop their vocabularies. Currently there is no guidance which the COIs or other MDR contributors follow with regard to defining their vocabulary elements or creating unambiguous definitions, making it all the more difficult to interpret the content.

Part 2 of the standard addresses how to manage and implement various classification schemes within an MDR, and how to classify administered items according to these schemes. While taxonomies seem to be the de facto data element classification scheme used by most COIs, there are other classification schemes to include ontologies, key words, and thesauri. One or more classification schemes may be used within a metadata registry to convey semantic content that is incompletely specified by other attributes such as names and definitions, adding to the richness of information available within the registry.

Finally, Part 6 of the standard addresses administration and maintenance of a metadata registry and could prove helpful in addressing some of the process and management issues associated with the MDR. Of interest in Part 6 are the required attributes for administered items (from Part 3), suggested registration status levels and criteria, suggested roles and responsibilities for operating a metadata registry, a concept of operations, and specific procedures for review and harmonization of administered items.

5.2 Common Reference Models

One of the most common questions regarding the application of ISO/IEC 11179 – or any other metadata approach – is whether the approach still requires data engineering as described in [27] and the use of common information exchange models, such as the C2IEDM/JC3IEDM.

The short answer is "Yes." One still needs data engineering, and the use of ISO/IEC 11179 is not a replacement for C2IEDM/JC3IEDM or other common data models/information exchange models. Conversely, using a common data model or information exchange model does not obviate the need for ISO/IEC 11179. This is because the domains of the two types of data standards are mutually supportive. While ISO/IEC 11179 addresses metadata and how it is described, organized, and managed in a metadata registry, data models categorize, structure, and describe the users' application domain. In the case of C2IEDM/JC3IEDM, the application domain is the battlespace.

The common denominator between the two is the real world concept that is being modeled. The *object classes* of ISO/IEC 11179 are references of real world ideas or concepts that are also modeled in the data models such as C2IEDM/JC3IEDM. Thus, the data model data elements (i.e., entities and relations) should also be reflected in the concepts modeled by the object classes of ISO/IEC 11179-3. This approach facilitates data mediation across disparate data models as long as all of the data models are mapped back to the ISO/IEC 11179-3 object classes in the metadata registry. Using this approach, if two COIs are using different data models – e.g., the one community agrees on the C2IEDM while another agrees to use the USSOCOM Common Database (CDB) – the relationship between the data can still be inferred as long as the describing metadata for each follows ISO/IEC 11179-3. What will differ is the structure of the object classes (compare Figure 9). The structure of the metadata will support the generation of data mediation data through mapping of the different object classes. This is the typical task of data managers in the process of data engineering (see [27]).

The current research on applications of the ontological spectrum, as introduced to SIW in [28] and other papers and as currently discussed within the C-BML group, comes into play at this point as well. The ontological spectrum of the Semantic Web is an expressive, comprehensive, and powerful form of data engineering. It is not a radically new concept, but it builds on traditional data modeling techniques and combines and transforms them into powerful ways of expressing rich relationships in a more thoroughly understandable manner. ISO/IEC 11179-3 can be seen as a first step to capture descriptions of terms of an application domain to enable higher overarching structures, such as thesauri, taxonomies, or eventually ontologies. A complete treatment of this topic goes beyond the scope of this paper, but this discussion illustrates the necessity to align metadata standards and repositories as soon as possible in order to avoid stove-piped metadata approaches standing in the way of data interoperability.

5.3 Metadata and the DoD Architecture Framework

The DoD Architecture Framework does not address metadata in their overview documents [35]. However, a closer look at Volume II: Product Descriptions [36], shows that the gap between ISO/IEC 11179 and DoDAF recommendations for the DoD Core Architecture Data Model (CADM) is surprisingly small. DoDAF requests a logical data model (operational view OV-7) and a physical data model (SV-11). The operational view specifies the logical information exchange between the operational nodes; the physical data model specifies how this logical view is implemented as messages or other protocols to exchange data between the systems. The CADM captures not only the data model, but describes every data entity with its domain and its value sets, attributes, and associations. The meta-elements recommended to do this can be mapped easily to the concepts dealt with in the other sections of this paper. In other words: if the logical data model and the physical data model are documented in OV-7 and SV-11, we already have a metadata model close to the recommendations given in this paper.

6 Summary and Conclusion

Data interoperability has been an objective of the DoD for as long as automated systems have been in existence, particularly in the area of Command and Control (C2). Data interoperability is critical to achieving higher levels of organizational interoperability that are required for an effective Joint Force that is increasingly dependent on IT in the new era of Net-Centric Operations and Warfare. Long time DoD efforts to achieve data interoperability through DoDD 8320.1 data element standardization efforts were not successful due to a variety of reasons, and these efforts have been superceded by the 2003 DoD Net-Centric Data Strategy and DoDD 8320.2. This approach seeks to capitalize on successes in the commercial IT sector through the use of web-based technologies and the concept of Service Oriented Architecture (SOA). The key to this approach is the metadata that describes the data and services being shared. Several DoD Communities of Interest (COI) are now producing and publishing metadata artifacts in the DoD Metadata Registry. Programs of Record participating in these COIs are also beginning to use these artifacts to expose their data via web services in various experiments and exercises.

While the Net-Centric Data Strategy is a powerful concept and much progress is being made, there are shortcomings that must be addressed. Some of these shortcomings are management-related and will be solved by efforts such as the Warfighter Mission Area COI governance body, the management of C2-related COIs as part of USJFCOM's C2 CPM responsibilities, and various efforts of the DoD CIO, DISA, Services, and others. Other shortcomings are more fundamental and are related to the metadata and the structure, organization, and management of the DoD Metadata Registry, which is the very foundation of the Net-Centric Data Strategy. ("It's all about the metadata".) While the current approach to metadata will ultimately make data visible and accessible to the enterprise, the data is currently only truly understandable and interoperable within a COI. Data understanding and interoperability across COIs remains a manual, ad-hoc process, and "on-the fly" machine-to-machine data interoperability and composition of services cannot be supported. In order to improve current efforts to implement the DoD Net-Centric Data Strategy and move toward the level of interoperability that is required for dynamic data exchange and composition of services, it is necessary to rethink how metadata is defined, organized, and managed.

This paper proposed an approach for "next-generation" implementation of the DoD Net-Centric Data Strategy that includes a comprehensive metadata repository exposing all the details of the data's definition and the mapping of this data through the systems that generate the standardized transactions. Specifically, an ISO/IEC 11179-3 compliant Metadata Registry is endorsed, with the metadata registry artifacts integrated into a distributed and federated metadata repository environment. Adoption of 11179-3 for metadata registries allows for higher levels of data interoperability as indicated in the LCIM because an ISO 11179 data element is defined within the context of concepts, conceptual domains, data element concepts, and value domains. These are all independent of the precise contextual restrictions that are imposed by an actual database table, as was the case with DoDD 8320.1 approaches to data interoperability. Consequently, ISO 11179 data elements can be defined at a much higher level of abstraction. ISO 11179-3 data element representations can support LCIM levels 4 and 5 and may also build the foundation for higher methods in the ontological spectrum.

If these advances are made then the benefits of XML and SOA can be realized because they will be founded on a basis of semantic harmony that corresponds to high levels of the LCIM. The role of SISO definitely starts in the C2/M&S Services forum and in supported study groups and product development groups. As stated in earlier papers, among others [29], the needs and requirements of M&S services are unique and must be brought to the table of GIG standardization as quickly and efficiently as possible.[10]

7 *Caveat*

This paper summarizes the main results of an independent study conducted by Leslie Winters as a Ph.D. student in the ODU M&S program. Andreas Tolk mentored the work and contributed several research papers. Mike Gorman supported the study with numerous white papers and his expertise in form of emails and discussions. As such, this paper is a product of academic work and does not necessarily reflect the official viewpoint of the organizations the authors work for.

8 References

[1] Government Accounting Office, Report GAO/NSIAD-87-124: DoD's Efforts to Achieve Interoperability Among C3I Systems, April 1987

[2] Assistant Secretary of Defense for Command, Control, Computers and Intelligence, DoD Directive 4630.6 Compatibility, Interoperability, and Integration of Command, 1992

[3] Starr, Stuart H. (2005) *The Challenges Associated with Achieving Interoperability in Support of Net-Centric Operations.* Proceedings of the 10th Command and Control Research and Technology Symposium, McLean, Virginia, June 2005.

[4] Chairman of the Joint Chiefs of Staff, U.S. Department of Defense: "Joint Vision 2020," Defense Technical Information Center, http://www.dtic.mil/

[5] U.S. Joint Forces Command: Capstone Requirements Document Global Information Grid (GIG), 30 Aug 2001

[6] Papazoglou, M.P. and Georgakopolous, D. *Service Oriented Computing* Communications of the Association for Computing Machinery, Volume 46 Number 10, OCT 2003

[7] Department of Defense Chief Information Office: Department of Defense Net-Centric Data Strategy, May 2003

[10] Readers interested in more practical applications are directed towards the Whitemarsh Website [30] for examples.

[8] ISO/IEC 11179 (2004). *Information technology – Metadata registries (MDR)*, Part I-VI, http://metadata-standards.org/11179

[9] Chairman of the Joint Chiefs of Staff, U.S. Department of Defense: "Joint Publication 1-02, DoD Dictionary of Military and Associated Terms," 12 April 2001 (as amended through 30 November 2004)

[10] Clark, T. and Jones, R. (1999) *Organisational Interoperability Maturity Model for C2*. Proceedings of the 4th Command and Control Research and Technology Symposium, U.S. Naval War College, Rhode Island

[11] Levels of Information Systems Interoperability, C4ISR Architectures Working Group, 30 March 1998, available at: US DoD, OSD (C3I), CIO, Director for Architecture and Interoperability Website. http://www.c3i.osd.mil/org/cio/i3/

[12] Tolk, A. and Muguira, J.A. (2003). *The Levels of Conceptual Interoperability Model (LCIM).* Proceedings IEEE Fall Simulation Interoperability Workshop, IEEE CS Press

[13] Turnitsa, C.D. (2005). *Extending the Levels of Conceptual Interoperability Model.* Proceedings IEEE Summer Computer Simulation Conference, IEEE CS Press

[14] Davis, P.K. and Anderson, R.H. (2003). *Improving the Composability of Department of Defense Models and Simulations.* RAND Corporation

[15] Page, E.H., Briggs, R., and Tufarolo, J.A. (2004). *Toward a Family of Maturity Models for the Simulation Interconnection Problem.* Proceedings of the Spring 2004 Simulation Interoperability Workshop, IEEE CS Press

[16] Andreas Tolk, "What Comes After the Semantic Web - PADS Implications for the Dynamic Web," *PADS*, pp. 55-62, 20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06), 2006, http://doi.ieeecomputersociety.org/10.1109/PADS.2006.39

[17] DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 1964

[18] Assistant Secretary of Defense for Command, Control, Computers, and Intelligence (ASD(C3I)), DoD Directive 8320.1, "DoD Data Administration," September 1991

[19] DoD Chief Information Office, DoD Directive 8320.2, "Information Sharing in a Net-Centric Department of Defense," December 2004

[20] DoD Chief Information Office, DoD Directive 8320.2-G, "Guidance for Implementing Net-centric Data Sharing," April 2006

[21] United States General Accounting Office, "Defense IRM: Management Commitment Needed to Achieve Defense Data Administration Goals", GAO-AIMD-94-14, 1994

[22] Chairman of the Joint Chiefs of Staff, Draft Instruction 8410.01, "Warfighter Mission Area Portfolio Management and Data Sharing," July 2006

[23] Chairman of the Joint Chiefs of Staff, Instruction 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems," March 2006

[24] DoD Community of Interest Directory, https://gesportal.dod.mil/sites/coidirectory

[25] FGM Incorporated, "Department of Defense Metadata Registry and Clearinghouse Version 5.2 User's Manual," http://metadata.dod.mil

[26] Semy, S. et al. (2005) "DoD Metadata Registry Recommendations," MITRE Technical Report 05B0000086, MITRE Center for the Air Force C2 Systems, Oct 2005

[27] Tolk, A. and Diallo, S.Y. (2005). *Model Based Data Engineering for Web Services.* IEEE Internet Computing 9 (4): 65-70

[28] Tolk, A. and Blais, C.L. (2005). *Taxonomies, Ontologies, and Battle Management Languages – Recommendations for the Coalition BML Study Group.* Proceedings IEEE Spring Simulation Interoperability Workshop, IEEE CS Press

[29] Winters, L.S. and Tolk, A. (2005). *The Integration of Modeling and Simulation with Joint Command and Control on the Global Information Grid.* Proceedings IEEE Spring Simulation Interoperability Workshop, IEEE CS Press

[30] Whitemarsh website http://www.wiscorp.com

[31] Hayes, G. (2006), DoD Metadata Registry Status Briefing to XML Community of Practice 17 May 2006, available at http://www.xml.gov/presentations/dod/mdr.ppt

[32] Department of Defense, Quadrennial Defense Review Report, 6 Feb 2006, available at http://www.defenselink.mil/qdr/report/Report20060203.pdf

[33] Assistant Secretary of Defense for Networks, Information, and Interoperability, DoD Directive 5100.30, Command and Control, 5 Jan 2006

[34] DoD CIO, *Implementing the Net-Centric Data Strategy Progress and Compliance Report*, draft version 10.3, 5 Jun 06

[35] Department of Defense Architecture Framework Working Group, Department of Defense Architecture Framework Version 1.0, 9 Feb 2004

[36] Department of Defense Architecture Framework Working Group, Department of Defense Architecture Framework Version 1.0 Volume 2: Product Descriptions, 9 Feb 2004

Author Biographies

LESLIE WINTERS is the Chief of the U.S. Joint Forces Command Net-Centric Information Integration Division, J6I. She is currently a Ph.D. student in the Old Dominion University Modeling and Simulation program and holds a B.S. and M.C.S. in Computer Science from the University of Illinois and an M.E. in Modeling and Simulation from ODU.

MICHAEL M. GORMAN is Senior Technologist at the Whitemarsh Information Systems Corporation of Bowie, Maryland. He has over 40 years in information technology. His specialties are databases, DBMS, data- and meta-data management. He is a co-author of the ISO/ANSI SQL standards for 1986, 1989, 1992, 1999, and 2003. He has been designing, and implementing methodologies, large scale database projects for 35 years, and has recently created a metadata repository that includes the ISO 11179 standard for data elements metadata.

ANDREAS TOLK is Associate Professor in the Faculty for Modeling, Simulation, and Visualization at the Engineering Management Department of the College of Engineering and Technology at Old Dominion University (ODU) of Norfolk, Virginia. He has over 16 years of international experience in the field of Applied Military Operations Research and Modeling and Simulation of and for Command and Control Systems. He is affiliated with the Virginia Modeling Analysis & Simulation Center (VMASC). His domain of expertise is the integration of M&S functionality into real world applications based on open standards. He received a Ph.D. and an M.S. in Computer Science from the University of the Federal Armed Forces in Munich, Germany.