Joint Doctrine Ontology: A Benchmark for Military Information Systems Interoperability

Peter Morosoff
E-Maps, Inc.,
Fairfax, VA
peter.morosoff@e-mapsys.com

Ron Rudnicki
CUBRC
Buffalo, NY
rudnicki@cubrc.org

Jason Bryant
Air Force Research Lab
Rome, NY
jason.bryant.8@us.af.mil

Robert Farrell
Air Force Research Lab
Rome, NY
robert.farrell.10@us.af.mil

Barry Smith
University at Buffalo
Buffalo, NY
phismith@buffalo.edu

***Abstract*—When the U.S. conducts warfare, elements of a force are drawn from different Services and work together as a single team to accomplish an assigned mission on the basis of joint doctrine. To achieve such unified action, it is necessary that specific Service doctrines be both consistent with and subservient to joint doctrine. But there are two further requirements that flow from the ways in which unified action increasingly involves not only live forces but also automated systems. First, the information technology that is used in joint warfare must be aligned with joint doctrine. Second, the separate information systems used by the different elements of a joint force must be *interoperable*, in the sense that data and information that is generated by each element must be usable (understandable, processable) by all the other elements that need them. Currently, such interoperability is impeded by multiple inconsistencies among the different data and software standards used by warfighters. We describe here the on-going project of creating a Joint Doctrine Ontology (JDO), which uses joint doctrine to provide shared computer-accessible content valid for any field of military endeavor, organization, and information system. JDO addresses the two previously-mentioned requirements of unified action by providing a widely applicable benchmark for use by developers of information systems that will both guarantee alignment with joint doctrine and support interoperability.**

Keywords—joint doctrine, military doctrine, ontology, Basic Formal Ontology (BFO), Common Core Ontologies (CCO), joint warfare, unified operations, interoperability, terminology, definition

I. Joint Doctrine

The publications of joint doctrine document fundamental principles and overarching guidance for the employment of the Armed Forces of the United States [1]. Joint doctrine applies to all military, from the joint staff to commanders of combatant commands, their supporting commands, and to the individual Services, each of which has its own Service-specific doctrinal publications. Joint doctrine is authoritative in the sense that, if conflicts arise between it and Service doctrine, then the former – absent more current and specific guidance from the Chairman of the Joint Chiefs of Staff – will take precedence.

Joint doctrine provides the benchmark for interoperability of the separate Service doctrines. And because all Service-level terminology is dependent on joint doctrine it is critical, if we are to prevent higher-level flaws cascading to domain-level doctrinal errors, that the terms of joint doctrine be defined correctly.

It is commonly supposed that doctrine provides not hard and fast rules but rather merely a loose and always revisable guide to action that is typically abandoned on first contact with the enemy. Doctrine is however authoritative also in the sense that it is to be followed in all cases except when, in the judgment of the commander, exceptional circumstances dictate otherwise. Moreover, there are many doctrinally acknowledged features of military action that survive through every engagement. Doctrine defines the shared frame of reference that remains active through every phase of every military engagement. This is because doctrine provides the principles that determine how to understand the authorized command relationships and the authority that military commanders can use. It establishes common ways of accomplishing military tasks and facilitates readiness by promoting coordination of training and planning. Most importantly for our purposes here, doctrine provides a common lexicon – a set of precise terms and precise definitions – expressed in a language that is designed to enable consistent understanding by military leaders, planners and educators. Doctrine thereby enables the sort of effective communication among warfighters that is needed for unified action.

II. Battle Management Language (BML)

While doctrine has been developed and used thus far to satisfy the needs of human beings, it is increasingly understood that it must also satisfy requirements that come into play when information systems are brought to bear in military action. The language used by warfighters and codified in field manuals and doctrinal lexica still involves some of the ambiguities characteristic of all languages used by human beings. But such ambiguities can be tolerated where human beings are involved because humans can easily disambiguate the meanings of ambiguous terms in everyday contexts of use.

The very human-friendliness of the language used by warfighters brings an equal and opposite weakness, however, when information systems are involved. Computers have difficulties in interpreting the common language of human beings and in using contextual cues to resolve ambiguities. Attempts to overcome these difficulties

led in around 2000 to the conception of the Battle Management Language (BML) [2] that was designed to allow the description of a commander's intent in the sort of context-free way that would support processing by automated systems. The initial goal of BML was to create a unified and unambiguous representation of command and control (C2) doctrine as a 'systematic data model' [2]. BML was seen as thereby providing a unified framework that would not only remove ambiguities but also rectify the terminological disunities created through the continued dominance of disparate Service cultures and of the numerous communities of interest within those cultures [3].

III. Interoperability

BML continues as an active project [4]-[5], especially in the modeling and simulation community. The promised unambiguous representation of the content of C2 doctrine using BML has, however, not been achieved. Here, we take up once again the idea of formalizing joint doctrine by drawing on more recent developments in the field of ontology. Our target, however, is more modest. It is not to provide the resources to capture formally a commander's intent. Rather, we seek to capture in a computer-usable form the terminological content of joint doctrine in a way that will support the sort of interoperability that is needed where live forces need to engage in unified action with information systems.

Interoperability is defined in the Glossary of DoD Instruction (DoDI) 8330.01 [6] as:

> The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment.

Our hypothesis is that the creation of a Joint Doctrine Ontology (JDO) can provide a widely applicable benchmark for use by developers of information systems that will support rather than impede unified action by breaking down existing terminological silos of different Services and communities of interest.

In contrast to the BML, our alternative approach begins, not with defining a new language, but rather with the existing authoritative controlled vocabulary that is defined in Joint Publication 1-02, the *Department of Defense Dictionary of Military and Associated Terms* [7].

The JP 1-02 dictionary consists in its current version of some 2,803 terms drawn from some 81 approved doctrinal publications forming the Joint Doctrine Hierarchy (at http://www.dtic.mil/doctrine/doctrine/status.pdf). In effect, we are constructing JDO as a shadow of JP 1-02, incrementally adding definitional enhancements and further elements of logical regimentation, but in such a way that the ontology, and the dictionary that underlies it, remain synchronized with each other through future revisions of joint doctrine. In effect, JDO will provide a semantic enhancement of JP 1-02, and therefore also of the terminological content of the separate Joint Publications from which the terms and definitions of JP 1-02 are derived.

The Dictionary defines the standard U.S. military and associated terminology needed to enable the joint activity of the Armed Forces of the United States. As stated in the Preface signed by Vice Admiral William E. Gortney, Director of the Joint Staff, these military and associated terms, together with their definitions, constitute approved Department of Defense (DOD) terminology for general use by all DOD components. [7]

In multiple other joint publications, as well as in a series of DoD and Chairman of the Joint Chiefs of Staff instructions, it is required that all DoD initiatives, as well as all warfighters and warfighting organizations, should use a common terminology. In addition, instructions state that all IT intended for use in military operations should be designed from the beginning to be interoperable (paragraph 9b of Chapter 2, "Doctrine Governing Unified Direction of Armed Forces," JP 1 [1]). We believe that it follows from these instructions that all DoD IT efforts, insofar as they are intended for use in military operations, should be developed in such a way as to be interoperable with joint doctrine.

IV. Failures of Interoperability and Requirement for Effective Guidance to IT Developers in the Future

The need for interoperability of DoD information systems and for alignment of the data and information that enables military action has been recognized repeatedly and at the highest levels, and given today's and tomorrow's flood of digital data across networks this need is becoming ever more apparent.

For example, DoDI 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense" [8] requires that authoritative data sources (ADSs) be 'registered in the DoD Data Services Environment (DSE).'

The DoDI directs further that 'Data, information, and IT services will be made … interoperable throughout their lifecycles for all authorized users'. However, the instruction to achieve such interoperability – namely through 'enforcement of policy for DoD metadata that uses Government and industry metadata standards' – repeatedly fails in its goal. This is not only because the policy is formulated in a way that falls short of the required specificity, but also because, even where relevant standards exist, they have in almost all cases been created *ad hoc*, to address specific local needs. Thus they have not been built in the sort of coordinated, rule-governed way that would be needed to achieve interoperability.

The problem of overly weak requirements is illustrated also in the already mentioned DoDI 8330.01 on "Interoperability" [6], where it is stated that the information systems that DoD components use

> must interoperate, *to the maximum extent practicable*, with existing and planned systems (including applications) and equipment of joint, combined, and coalition forces, other U.S. Government departments and agencies, and non-

> governmental organizations, as required based on the operational context (italics added).

Because everything is by definition interoperable to 'the maximum extent practicable,' this instruction is without teeth.

DoDI 8320.02 suggests a further route to the achievement of interoperability through adherence to standards listed in the DoD IT Standards Registry (DISR). Unfortunately, it is difficult to determine the degree of interoperability of DISR standards, in part because the needed assessment must be applied simultaneously to the different portions of the DISR, and these often require different sorts of permissions (and thus, we assume, are accessible only to different sorts of people). Some of the resources contributed to the DISR that we were able to access, however, do not manifest – even when taken singly – the sort of minimal terminological consistency or formal regimentation that would be needed to meet the demands of interoperability. The terminology defined in [9], for example, was created by selecting terms and definitions from a wide range of sources. No common rules for definitions were employed, and so there is no way of checking even for simple logical consistency of the resulting artifact.

Achieving interoperability – both terminological and structural [10] – is of course difficult for a large organization like the DoD with a cumbrous history of information system development. However, in recent years a number of best practices for meeting the demands of inoperability have been established, some of them very simple to implement. Thus a first task would be to establish corresponding simple rules that must be satisfied by IT systems developed by the DoD in the future. We are concerned here only with issues of *terminological* interoperability, which we propose should be addressed through the creation of a benchmark ontology framework centered around the JDO. We envisage that the complementary *structural* interoperability might be tackled in part through the deployment of W3C standard resources such as RDF and the Web Ontology Language (OWL) [11]. The formulation of ontologies using OWL, in particular, would allow computational reasoners to be used in a way that provides automatic checking for consistency of definitions with each new revision of a terminological artifact such as JP 1-02. The ontology approach can thereby support agile development and coordinated maintenance of information systems in a way that does not sacrifice terminological interoperability [12]–[16].

V. The Solution

DoDI 8330.01 [6] already requires that *the content of joint operational concepts, and associated doctrine and operational procedures, address interoperability* of the IT used by the separate Services and also, where required, by joint and multinational forces and other U.S. government departments and agencies.

While DoD thus requires that joint doctrine addresses the need for IT interoperability, it crucially does not require – and has no effective strategy to ensure – that the IT systems and procedures themselves address the need for conformity with joint doctrine. We believe, however, that such conformity is not only indispensable if unified action between human warfighters and IT systems is to be achieved, but further that it would bring multiple significant benefits to military IT systems themselves, and thus also to the developers of such systems, because it would provide a benchmark for interoperability.

VI. Unified Action of Human Warfighters and Information Systems

JP 1, the Capstone Publication of Joint Doctrine [1], states that unified action demands 'maximum interoperability':

> The forces, units, and systems of all Services must operate together effectively, in part through interoperability. This includes joint force development; use of joint doctrine; the development and use of joint plans and orders; and the development and use of *joint and/or interoperable communications and information systems* (italics added).

Because a military organization includes its information systems, we believe that building the common language provided by doctrine into the information systems that will be used by warfighters is a vital need.

The DoD Manual (DoDM) 5120.01, "Joint Doctrine Development Process" [17], provides the guidance that steers DoD to consistent terminology across the joint publications governing different types of operational domains. Developers of doctrine are required to 'use, to the greatest extent possible, previously approved terminology contained in the text of other JPs or in … JP 1-02.' An information system needs more than well-trained and qualified people and high-quality equipment to provide effective support to unified action. It must be supported also by effective guiding principles and procedures rooted in an understanding of the requirements of unified action. Our proposal is that such support can be achieved in today's networked environment by extending the same guidance that is provided to doctrine developers also to IT developers. Those engaged in developing IT systems for military operations should be required to take the terminology and definitions of joint doctrine as their starting point. Increasingly, if this proposal is adopted, doctrine developers will come to be seen as constituting the first rank of information technologists, providing the core terminological content on which all DoD IT content will rest.

VII. Rules for Definitions in Instruction 5705.01D

To see how JDO will be constructed, we need first to understand some of the features of the Dictionary from which it will be derived. The idea for such a dictionary is expressed in DoDI 5025.12 of August 2009 [18], which states that it is DoD policy to improve communications and mutual understanding within the DoD, with other Federal Agencies, and between the United States and its international partners through the standardization of military and associated terminology.

This position is restated in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5705.01D of November

10, 2010 on the creation of a "Standardization of Military and Associated Terminology." [19] Specifically, the Chief of the Joint Education and Doctrine Division (JEDD), J-7, shall oversee the DoD Terminology Program and U.S. participation in the NATO Terminology Programme; serve as Joint Staff planner for terminology issues; and appoint and supervise the Joint Staff terminologist.

Enclosure C of this instruction provides a "Definition Writing Guide," which includes a specification of the scope of JP 1-02 and also simple rules for writing definitions. Such rules are of obvious importance for our needs here, since an ontological counterpart of JP 1-02 can be created only if the definitions contained in the latter are in good order from the point of view of logical consistency.

As concerns scope, the Guide specifies that the Dictionary will include terms of general military or associated significance. Technical or highly specialized terms may be included if they can be defined in easily understood language and if their inclusion is of general military or associated significance. The Guide requires further that the dictionary be non-redundant: thus, a term will be added to the dictionary only if '[an] approved joint term with similar definition does not exist.'

The Guide defines a definition as 'a formal statement of the exact meaning of a term that enables it to be distinguished from any other.' A definition is distinguished from a description by the fact that the latter 'is a narrative containing information about the term that is not constrained in format or content.'

Principles for the development of a definition require that it should be:

Clear – Address the meaning of the term only. A definition should not contain doctrinal or procedural information; i.e., it should focus on describing "what" a term is and not "how" or "why" it is used.

Concise – Be as brief as possible, including only information that makes the term unique. Limit the definition to one sentence whenever possible.

Complete – Include all information required to distinguish the term from those that are related or similar.

The Guide includes also a list of types of errors that are to be avoided when writing definitions. For example, a definition should not be *over-restrictive*; it should not be *circular*; it should be *positive* (state what is covered by a term rather than what is not covered); and it should contain no *hidden definitions* (where the definition of one term is embedded inside another).

The rules codified in the Guide conform very well to the best practices identified by terminologists who have studied the authoring of definitions [20]. That violations of these rules have slipped though the coordination process, however, is seen in the fact that errors of each of the mentioned kinds can still be found (see Table 1).

Avoiding these and other types of errors would not only make JP 1-02 more valuable to human users; it would also enable the construction of the formal representations of its content of the sort that are needed for use in computational systems. We have already proposed a series of supplementary rules for the formulation of definitions (summarized in [12]), rules which have been tested in some 150 ontology initiatives over a wide variety of domains (see under 'Users' at [14]). We are applying these rules in building the JDO, thereby providing a vehicle that can support the usage of joint terminology by computers without sacrificing understandability by humans. These definitions can also be of help in the process of revising joint publications in the future, allowing the content of JP 1-02 to be used as part of a computational process of quality assurance for the use of terminology in joint publications when successive revisions are made.

	U	N	C	H
operational area =def. An overarching term encompassing more descriptive terms (such as area of responsibility and joint operations area) for geographic areas in which military operations are conducted.	x	x		x
contingency operation =def. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (Title 10, United States Code, Section 101[a][13])			x	
subordinate command =def. A command consisting of the commander and all those individuals, units, detachments, organizations, or installations that have been placed under the command by the authority establishing the subordinate command.		x	x	

Table 1: Examples of errors in JP 1-02 (from June 15, 2015)
U = **unclear,** N = **not concise,** C = **circular,** H = **hidden definitions**

VIII. Proposed Supplementary Rules for Definitions

We provide five examples of such rules, and illustrate their application to creating the JDO.

Rule 1: *Do not confuse the entity you are defining with the term used to represent that entity.*

(Failure to heed this rule is illustrated in the definition of **operational area** in Table 1 – an operational area is not a 'kind of overarching term'.)

Rule 2: *Distinguish between general terms and proper names.*

Almost every JP 1-02 term is a general term, which is to say, it is a term that refers to something general – a kind or type (as in all the cases listed in Table 1) – having multiple specific instances. A small number of JP 1-02 terms are proper names, which is to say, they refer to exactly one specific instance. Examples include the **Universal Joint Task List** and **Joint Doctrine Development System**. Such terms are standardly marked by use of initial capitals, but their treatment in JP 1-02 is sometimes uncertain. The definition of **Army air-ground system**, for instance, suggests that there is exactly one Army air-ground system, so that 'Army air-ground system' would be a proper name.

However, there may be a plurality of such systems used by the Army at any given time.

Rules 3–5 apply only to general terms, and are satisfied already by the definitions of many such terms in JP 1-02:

> Rule 3: *All general terms should be singular in number*.
>
> Rule 4: *Each general term should have at most one single parent term.*
>
> Rule 5: *The definition of each general term* A *should specify the associated parent term* B *and state what it is about the* A*s that marks them out from all other instances of* B *as instances of* A.

Thus a definition of a general term A should have the two-part form:

> An A =def. a B which Cs.

For example (from [16]):

> **artillery vehicle** =def. A *vehicle* which *is designed for the transport of one or more artillery weapons.*
>
> **artillery weapon** = def. A *device* which *is designed for projection of munitions beyond the effective range of personal weapons.*

Returning to JP 1-02 we can now, following rule 5, define:

> **operational area** =def. A *geographic area* in which military operations are conducted. (Contrast the first row of Table 1.)

Here 'geographic area' is the parent term; the specific difference is 'in which military operations are conducted.' The overwhelming majority of JP 1-02 definitions are already of this form. Consider for example:

> **theater of operations** =def. An operational area defined by the geographic combatant commander for the conduct or support of specific military operations.

Many of the remaining cases are easily converted to be of this form without any change of meaning. Starting, for example, from the definition:

> **cyberspace operations** = def. The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Here two conversion steps are needed. The first replaces the term to be defined with a singular noun following rule 2. The second, in accordance with rule 5, adds a representation of the appropriate parent term (here, trivially, **operation**) to yield:

> **cyberspace operation** =def. An operation that employs cyberspace capabilities and has primary purpose: to achieve objectives in or through cyberspace.

Such rules may seem trivial, and the effect of their application may be very slight when measured against the understandability and utility from the point of view of human beings of the definitions to which they give rise. But they bring two immediate benefits when IT systems are brought into play. First, because IT developers lack warfighters' experience and therefore context, they need definitions with as little ambiguity as possible. And second, the changes proposed bring aid not only to the formalization of joint doctrine terminology in the JDO – where adherence to rule 5 allows immediate generation of the backbone taxonomy of the ontology – but also to the quality assurance of joint doctrine definitions themselves, by allowing easier checking of logical consistency.

IX. Building the JDO

A. The OBO Foundry

Our strategy for building the JDO follows an approach to coordinated ontology development as a means to advancing interoperability across multiple domains that was first successfully applied in the life sciences in the context of the Open Biomedical Ontologies (OBO) Foundry initiative ([21]). The strategy rests on dividing the domain of biomedicine into a number of sub-domains (for genes, proteins, cells, and so forth) and creating ontology modules representing the corresponding general types of entities. Each ontology module consists of general terms organized hierarchically through the parent-child relation between types and subtypes. This relation then serves as the starting point for the formulation of the definitions of the terms in the hierarchy in accordance with Rule 5 above. This strategy is currently being applied in a series of DoD and intelligence community projects, in each case drawing on the Basic Formal Ontology (BFO) [12], which serves as a common upper level starting point for the creation of definitions of the terms used in the domain ontologies at lower levels.

The predominance of general terms in JP 1-02 reflects the purpose of military doctrine, which is to help warfighters understand the realities of war and their specific situations. It achieves these ends largely through the identification and explanation not of specific instances (such as a particular aircraft or IT system) but rather of important general categories. Doctrine is re-usable because it is applicable to many different instances and to many different sub-kinds of the same general categories that re-appear in ever new situations. This approach is effective because the basic realities of war are not changed by the fielding of new commanders, equipment, specialties, or tactics. A new IT system may provide a commander with more information in easier-to-understand formats; but the basic role of IT in supporting unified action remains unchanged. Because the developers of doctrine were so successful in identifying the high-level categories of C2, commanders and others continue to use these same categories when understanding how to employ each new IT system to create better operational capabilities.

The most general categories in military doctrine are:

(1) *thing* (people, equipment, organizations),

(2) *attribute* (capabilities, functions, roles, including relational attributes of command or support), and

(3) *process* (for example, the joint planning process).

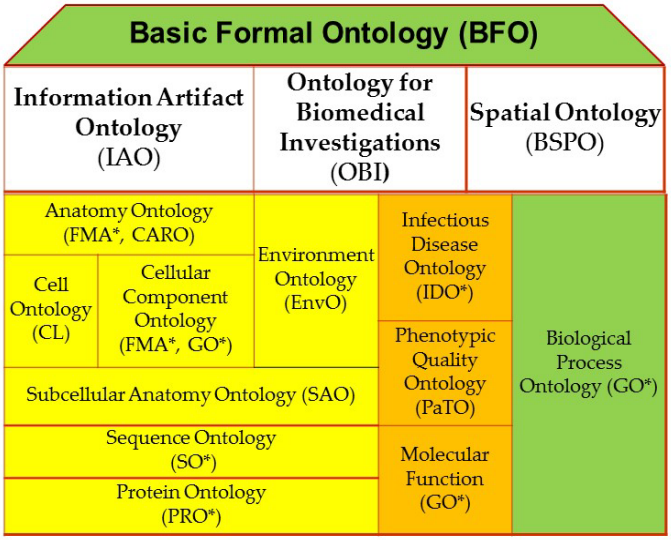

Figure 1: OBO Foundry strategy for modular coordination

Nowhere is it stated explicitly in military doctrine that these are the basic categories of the reality of war. Rather, the doctrinal publications are divided by area of warfare and by process (C2, intelligence, fire support, logistics, planning, and so forth). One of the virtues of joint doctrine is its consistent use of the same general terms representing sub-categories of *thing*, *attribute*, and *process* across all the joint publications. For example, every joint publication uses the term **commander** (*thing*) for the officer appointed to **command** (*process*) an **organization** (*thing*) and to exercise **authority** (*attribute*) over subordinates. It is impossible to understate the value of this achievement, which has not only diminished communications barriers among the warfighters of different specialties but also facilitated the application of IT in planning, training, and real world operations. What is remarkable is that the authors, managers, and terminologists of joint doctrine achieved this consistency with minimal documented theory and procedures for categorization and for the writing of definitions.

B. *BFO and the Common Core Ontologies*

In our view, BFO provides the documented theory needed to fill this gap [12]. BFO is architected around the same upper-level categories (of *thing*, *attribute*, and *process*) used by joint doctrine. More importantly, BFO serves as the starting point for a suite of associated resources – based on the Common Core Ontologies (CCO) (see [11] and Figure 2) – that have been purpose built to support IT applications in the military and intelligence domains.

The CCO and other domain-ontology modules are (1) defined in BFO terms and then (2) they are themselves extended through the addition of domain-specific sub-ontologies along the lines illustrated in Figure 2. The BFO community has refined and tested the needed theory and procedures for generating such sub-ontologies in agile fashion and for preserving their usability and mutual consistency across successive versions. [14]-[16].

C. *Building the JDO as Shadow JP 1-02*

Our strategy for building JDO is incremental. We proceed through the successive joint publications (JP n-m), moving from general to specific, for instance from JP 3-0 (*Joint Operations*) to JP 3-14 and JP 3-17 (*Space Operations* and *Air Mobility Operations*). The creation of an ontology for each JP n-m then follows three steps:

i. ENRICHMENT: create JP n-mE, a shadow version of those portions of JP 1-02 whose terms are defined in JP n-m but enriched (E) through the addition of new terms – for example, **commander** – that are not defined in JP 1-02 but used in JP n-m definitions;

ii. LOGICAL REGIMENTATION: create JP n-mLR, a logically regimented (LR) version of JP n-mE, in which definitions are formulated in humanly understandable English but with the logical regimentation sketched in our summary treatment of supplementary rules for definition writing in section VII, as supplemented by the further rules set forth in [12]);

iii. FORMALIZATION: create JP n-mF, in which the human-readable definitions in JP n-mLR are formalized (F) using the Web Ontology Language (OWL);

Content from CCO is incorporated in each stage as needed. Examples are provided at http://ncor.buffalo.edu/JDO-Oct-2015.

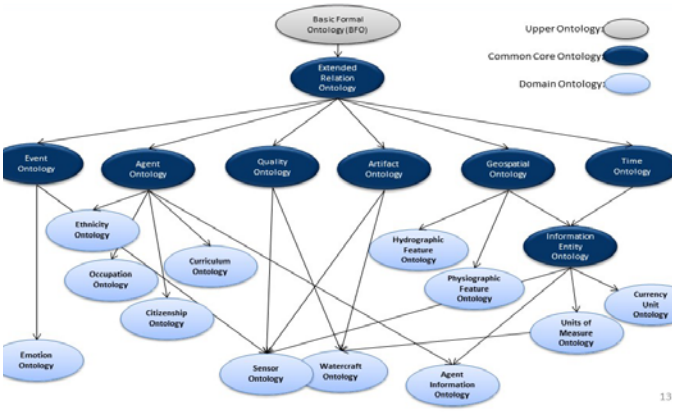

Figure 2: Common Core and associated domain ontologies

X. POTENTIAL BENEFITS OF THE JDO TO THE WARFIGHTER

We are developing the JDO to support efforts to extend the applicability of doctrine in those areas where commanders, planners, and other warfighters need to call upon information and information support in order to be effective. JDO will provide a computationally accessible counterpart of the content of JP 1-02 designed to support unified action by advancing terminological consistency and interoperability.

The major benefit of JDO should take the form of better C2 through improved communication, self-synchronization, and projection into the future, and in each stage of development of the JDO we will be testing its utility in supporting improvements along all of these dimensions.

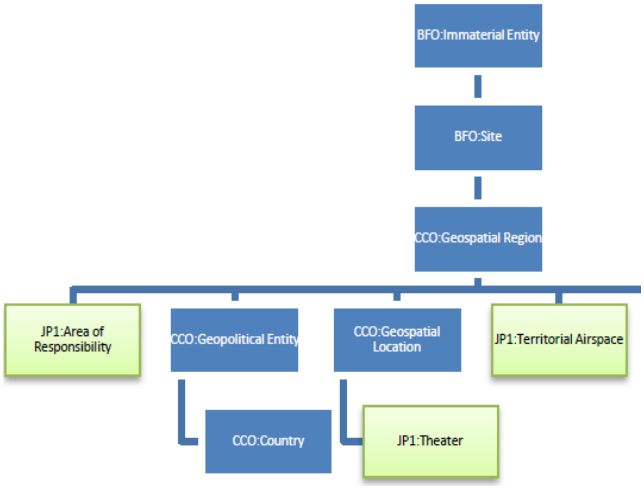

Figure 3: Examples of CCO and JP 1 terms descending from BFO in the JDO

As stated in JP 6-0 ("Joint Communications System") [13], a C2 system has two elements: (1) the people, who make decisions and accomplish missions, and (2) the facilities, equipment, communications, staff functions, and procedures essential to the commander for C2. People can conduct C2 without facilities, equipment and so forth, but the latter cannot perform C2 without people. Since unified action occurs not only between people and organizations, but also between IT systems and people, by advancing interoperability in the ways described above, a successfully developed JDO can facilitate moving past the low level of unity of action among people, organizations, and IT systems that has been achieved until now.

A subsidiary benefit takes the form of providing ways to extend the range of IT-supported uses of the content of doctrine, for example, by allowing the DoD Dictionary to serve as an entry point for web-based searches across multiple repositories of authoritative data; by facilitating greater coordination of training and operations; and by increasing automation of processes such as plan specification, course of action development, and operations and Blue Force Status assessment, particularly within highly contested environments.

We anticipate that the JDO will allow further enhancements of JP 1-02, for example, by providing for each term in the dictionary its own web page that can serve as a repository of usage and of revision history. This last benefit is part of our more general strategy to assist developers of the hundreds of IT systems that are developed for U.S. military operations to achieve the benefits of interoperability and to keep track of needed information.

Access to detailed information on the usage and revision history of the vocabularies of the intended users of these hundreds of systems would facilitate unified action among IT developers, for example, by helping to rectify the current situation in which even the best-intentioned and conscientious IT developers must make assumptions on whether a warfighting term in a specification that is listed in joint doctrine is intended to be defined by the current or by some previous definition in JP 1-02. Integration of the JDO within the larger BFO–CCO framework would also help to resolve some of the problems that arise when expressions are used in JP 1-02 definitions but are themselves not defined in JP 1-02.

XI. Potential Benefits of JDO to the Doctrine Staff

Anticipated benefits of JDO to *doctrine authors* include the ability to apply standard ontology editing and visualizing software, for example, to create visualizations of how different parts of doctrine interact, of the doctrinal content relevant to particular types of operations or capabilities, or of the ways doctrine is used (and not used) in specific plans and operations. These benefits include opportunities for logical tracking of dependences among terms and definitions to identify (direct and indirect) circularities and thereby to help to ensure, when changes in definitions are made in the process of revision, that the effects of these changes cascade appropriately through all dependent definitions.

For example, imagine that revisions need to be made to the definition of a term such as **base defense** illustrated in Figure 4. The Figure tells us which definitions then need to be checked for continued validity, by showing the terms in JP 1-02 that are defined using **base defense** either directly or indirectly (by inheritance from a definition lower down the corresponding chain).

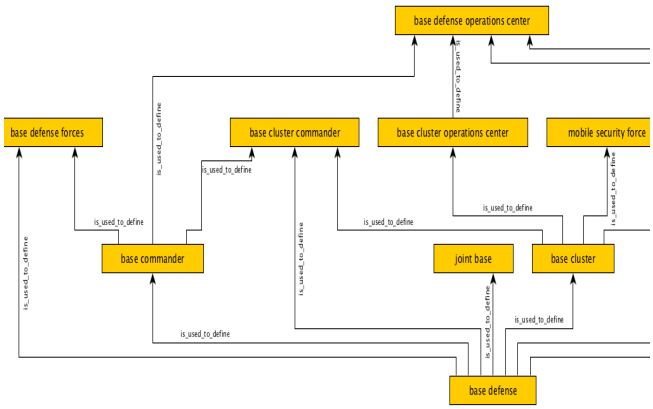

Figure 4: Fragment of the JP 1-02 network generated by the relation *is used to define.*

We believe that terminological interoperability can be achieved only where the terminologies involved are developed as part of, or are defined in terms derived from, a common benchmark ontology framework. Only such a framework can provide a basis for clearly formulated logical relations between terms, and only this will allow the sort of automated checking for consistency that is needed when the terminological content of multiple information systems is aggregated together in larger (actual or virtual) systems. This requirement for automated consistency checking becomes all the more urgent as terminological artifacts are revised over time. We believe that the value of the JDO will reveal itself not least in supporting consistent revision of JP 1-02 in tandem not merely with Service and coalition doctrines but also with information artifacts such as the Universal Joint Task List (UJTL), the Joint Lessons Learned Information System (JLLIS), and their Service counterparts.

Finally, JDO can also help the many teams of ontologists working on different military and intelligence community initiatives to advance information discovery and processing. The JDO will enable doctrine to serve as a new source of ground truth for ontologists across DoD and IC that can help to ensure mutual consistency and identify wasteful redundancies as well as gaps and errors in existing ontologies. It will contribute to consistent and yet agile development of IT technology while also counteracting current tendencies toward silo formation and failures of interoperation.

APPENDIX: EXAMPLES OF PRIOR WORK

The practical value of an ontology-based approach to supporting operational military IT has been demonstrated most conspicuously in the ICODES (Integrated Computerized Deployment System) load-planning system, a program of record employed by the DoD since 1997 [22].

A more recent example is the AFRL (Air Force Research Lab)/USTRANSCOM Mission Data and Transport Ontology project described in [23]. Here, the goal was to create a domain model of U.S. Transportation Command's operations, including operational processes, organizations, and Commander's Critical Information Requirements (CCIR), to be used to support the monitoring of information relevant to USTRANSCOM missions. Specifically, rules were used to modify terms and definitions of the Joint Mission Essential Task List (JMETL) in ways similar to those described in section VIII in relation to the definitions of **operational area** and **cyberspace operations**. When the resulting domain model was used with the Securboration MetaTagger application, there was a reduction 20% in the numbers of people required for monitoring for critical information and a reduction of 1–3 days in discovering such information.

Another AFRL effort used analogous rules in transforming a portion of the Joint Capability Areas (JCA) taxonomy into an ontology-based model that was then processed by a machine-learning algorithm to train an application. Formalizations of the JCA descriptions were used to allow comparisons of unstructured text against each of the formalized descriptions in order to determine matches. Initial attempts to disambiguate each of the JCA descriptions failed because of redundancy and ambiguity. Instead, a hybrid was created consisting of formalizations of JCA descriptions along with word bags of their respective contents. A machine learning algorithm was then used to compare historical user input against both to train the algorithm. Here, too, the implementation (described in [24]) shows a reduction in 1–3 days for discovering critical information that could affect USTRANSCOM operations, for example, in case of earthquake or other disaster and a 20% reduction in manpower required for monitoring the information.

ACKNOWLEDGEMENTS

Our thanks go to Lieutenant Colonel James McArthur (USMC JS J7), Lieutenant Colonel William D. Betts (USAF JS J7), Tatiana Malyuta (CUNY), Tony Stirtzinger (Securboration), Andreas Tolk (MITRE/Old Dominion University), and Erik Thomsen (Charles River Analytics).

REFERENCES

[1] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, 25 March 2013.

[2] M. R. Hieb, S. Carey, M. Kleiner, M. Hieb, R. Brown, "Standardizing Battle Management Language – A Vital Move Towards the Army Transformation", *IEEE Fall Simulation Interoperability Workshop*, 2001.

[3] S. Lambert, M. R. Hieb, "Improving Unity of Effort in Command and Control Processes: An Operational Analysis of a Joint Doctrinal Language", *Spring Simulation Interoperability Workshop*, 2006, 743-752.

[4] Tolk, Andreas, and Curtis Blais. "Taxonomies, Ontologies, Battle Management Languages – Recommendations for the Coalition BML Study Group", Spring Simulation Interoperability Workshop 2005.

[5] Simulation Interoperability Standards Organization (SISO), Standard for: Coalition Battle Management Language (C-BML), Phase 1 SISO-STD-011-2012-DRAFT 4 April 2012.

[6] Department of Defense Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)", May 21, 2014.

[7] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, as amended through 15 June 2015.

[8] Department of Defense Instruction Number 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense", August 5, 2013.

[9] Acquisition Community Connection (ACC) Practice Center, Terms and Definitions, Open Systems Architecture, https://acc.dau.mil/Community Browser.aspx?id=220108&lang=en-US, October 14, 2015.

[10] J.-F. Ethier, O. Dameron, V. Curcin et al., "A unified structural/terminological interoperability framework based on LexEVS", *Journal of the American Medical Informatics Association*, 2013, 20, 986-994.

[11] J. R. Schoening, et al., "PED fusion via enterprise ontology," *Proceedings of SPIE 9464,* Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VI.

[12] R. Arp, B. Smith, A. D. Spear, *Building Ontologies with Basic Formal Ontology*, Cambridge, MA: The MIT Press, 2015.

[13] Joint Publication (JP) 6-0, *Joint Communications System*, June 2015.

[14] Basic Formal Ontology, http://ifomis.org/bfo, September 2015.

[15] D. Salmen, T. Malyuta, A. Hansen, S. Cronen, B. Smith, "Integration of Intelligence Data through Semantic Enhancement", *Semantic Technology in Intelligence, Defense and Security* (STIDS), 2011, CEUR 808, 6-13.

[16] B. Smith, T. Malyuta, W. S. Mandrick, C. Fu, K. Parent, M. Patel "Horizontal Integration of Warfighter Intelligence Data. A Shared Semantic Resource for the Intelligence Community", *Semantic Technology in Intelligence, Defense and Security* (STIDS), 2012, CEUR 996, 112-119.

[17] Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5120.01, "Joint Doctrine Development Process," December 29, 2014

[18] Department of Defense Instruction 5025.12, "Standardization of Military and Associated Terminology," August 14, 2009.

[19] Chairman of the Joint Chiefs of Staff Instruction 5705.01D "Standardization of Military and Associated Terminology," Nov. 10, 2010.

[20] S. Seppälä. "An ontological framework for modeling the contents of definitions", *Terminology*, 21(1):23–50, 2015.

[21] B. Smith, et al., "OBO Foundry: Coordinated Evolution of Ontologies to Support Biomedical Data Integration", *Nature Biotechnology*, 25 (11), 1251-1255.

[22] K. Pohl and P. Morosoff, "ICODES: A Load-Planning System that Demonstrates the Value of Ontologies in the Realm of Logistical Command and Control (C2)", *InterSymp-2011*, 2011.

[23] J. M. Powers, Keith D. Shapiro, and David S. Monk, "Information Exchange and Fusion in a Collaborative Environment using Semantic Information Requirements", *International Conference on Collaboration Technologies and Systems* (CTS 2014). 597-601.

[24] Securboration, "Human assisted analysis for change alignment to an Enterprise Architecture", Requirements Analysis Portlet (RAP). May 2012.