

Command and Control Common Semantic Core Required to Enable Net-centric Operations

Mr. Erik Chaum

Naval Undersea Warfare Center
ChaumE@npt.nuwc.navy.mil

Mr. Richard Lee

DDR&E (Advanced Systems & Concepts)
Richard.Lee@osd.mil

Abstract

Commanders and decision makers require timely and accurate information. The power of information and information sharing are fundamental tenets of the ongoing defense transformation. Making information discoverable, accessible, and understandable are critical to achieving net-centric capability. Of these, the most difficult to accomplish is the requirement to make shared information "understandable". This paper discusses enabling shared understanding in the joint and multinational operational context and recommends leveraging the ongoing work of the Multilateral Interoperability Programme (MIP). It also looks at cost and performance factors.

1. Information is essential, and useful, if you understand it!

Commanders and decision makers require timely and accurate information. The power of information and information sharing are fundamental tenets of the ongoing defense transformation to net-centric / network-enabled operations. These ideas are age old. What is new, and motivating alternative concepts of operation and architecture changes, are emerging information sharing options and technologies. Net-centric information sharing guidance highlights the need to make information discoverable, accessible, and understandable[1]. "Discoverable" and "accessible" are today readily accomplished using industry standards and commercial technology. Of course the application of these capabilities must be engineered to suit the operational environment and requirements. Far more difficult to accomplish is the requirement to make shared information "understandable".

2. Net-centric concepts

Net-centric operational concepts seek to flatten, broaden and speed information sharing. Information sharing can occur between people, between "information systems"¹, and between people and information systems (or visa versa). When a human is the recipient of information (e.g., web page) we rely on his or her training and knowledge to process the information shared. We have seen the power of improved discovery, access and user interpretation in the revolution brought by internet search engine and web page technology. Net-centric operations require much more than discover and display. We must be able to share information among many types of warfighter systems and services such that it can be reliably processed in an automated manner. Necessarily, this includes data and relevant context², both of which are usually required to understand, reason and intelligently process. This relevant context is not limited to simple metadata (e.g., position uncertainty for position) but includes broader context knowledge about objectives, operational and tactical plans (e.g., orders, status, capabilities, control measures, rules of engagement, logistics, etc.), intelligence estimates, and natural and cultural environmental knowledge. Normalizing this data will simplify its processing, analysis and fusion. Mission software and services that are able to "understand" the broader set of relevant normalized information will provide better recommendations and capabilities to the warfighter.³

Net-centric operational concepts also seek to move power to the edge and in doing so empower the

¹ Information systems – meaning any type of networked software-based system, application or service.

² Information is often thought of as "data in context".

³ Even though a browser displaying information does not understand the content of the page, it understands and expects the content to be passed in a formal language, e.g., HTML.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 20 MAY 2008		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Command and Control Common Semantic Core Required to Enable Net-centric Operations				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Undersea Warfare Center				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 29	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

warfighter, who when better informed, is able to operate in a more agile, timely, and synchronized manner. For this reason also, net-centric operations require the sharing of both situation information and operational context type information, e.g., command intent – objectives, plans, orders, priorities. Sharing this knowledge helps to provide focus across the force, enables collaboration, and supports the decision making required to achieve convergence of effort[2]. Collaboration is likely to be more successful and efficient when the participants have a common understanding of the shared information and are working to decide what to do, and not spending their time trying to resolve discrepancies in their interpretations of the shared information.

3. Defense transformation and reengineering

Net-centric directives make the case that past coordination, acquisition, and integration practices have led to a complex mesh of generally *point-to-point*, and/or proprietary, information sharing capabilities (i.e., unique interface languages for specific systems)[1]. These have been expensive to build and maintain, and in a net-centric context, provide relatively limited information sharing or automated processing capability. A former US Marine Corps component C4 director during Operation Iraqi Freedom identified the problems of 1) uncertainty that information had been successfully communicated, 2) delay in translation and 3) ambiguity in interpretation, as the boundary conditions leading to a “psychological space” in which bad things happened[3]. Achieving more effective information sharing requires sharing a domain language, one that supports the warfighter's operational needs. System-specific unique languages and internal models are seldom equivalent, resulting in a “Tower of Babel” situation that limits sharing and shared understanding[4]. While translation (a.k.a., mediation) is possible, too often it causes the loss of precision, meaning, and or context⁴. Translation can, as a result, inject uncertainty and ambiguity further degrading the quality of information being shared. These losses are typically not shared with the decision maker! Maintaining the quality and context of information as it is being shared is critical to it being properly understood and subsequently used by the decision maker.

⁴ Admittedly, there are translations that are purely syntactic and lossless. However, this happens infrequently when translations are between independently developed models.

The US DoD Net-centric Data Strategy (NCDS) begins to address this problem with the establishment of Communities of Interest (COI). A COI is a “collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange.”[1]

The NCDS directs that COI be formed to break-down system and Service language barriers (stovepipes⁵). COIs are to establish consensus on operational processes, activities, and supporting data standards. This enables communities to evolve to a *many-to-many* approach to domain information sharing. Implementers gain a simplified set of common concepts, processes, business rules and “language”. The resulting conformant community systems and services are able to process and add value because they have been built to “understand” the community data. This consensus and standards-based practice is simply good open architecture systems engineering, if difficult. COIs alone are necessary but not sufficient in that they might only establish new bigger functional stovepipes and not address the basic interoperability problem at the joint level.

In the net-centric objective (to be) state we expect to have evolved to a lean collection of systems and services that 1) add value to warfighter defined community processes, 2) are loosely coupled, 3) speak common domain languages, and 4) follow prescribed business rules – enabling them to “plug-and-play” properly. A well-defined COI interoperability profile (published through an enterprise registry) defines for legacy systems how they must evolve and creates for new systems and services a clean community design baseline. As simple as this may sound, it should be noted that the horizontal integration required is not always supported by governance or funding processes, nor is the open architecture concept fully embraced by all industry partners.

4. Integrated mission capability

The well-defined community interoperability profile enables significant cost savings in a number of areas. The development of a shared language eliminates the development cost of many unique languages, the development of many unique translators, the associated testing and maintenance.

⁵ It should be noted that a COI encompasses a group that shares a type of information and is not limited to functional specialty systems (e.g., C2 systems that use logistics information and logistics systems need to share a common language for their information exchanges).

There is an implied requirement to investment in the COI process and language definition, language training for implementers, governance and accreditation. Current operational costs (due to information losses, ambiguity and uncertainty) may be high but are difficult to quantify. The value of interoperability improvements to warfighter community processes, thanks to ubiquitous automated processing, are likely high and somewhat easier to quantify.

A recent DoD Information Sharing Strategy memorandum notes that there are "numerous independent mission or functional area specific initiatives addressing aspects of information sharing." It goes on to say that "these strategies and efforts must be synchronized in order to achieve unity of effort as well as economic and operational efficiencies".[5] What must we do to ensure that warfighter processes are not "islands of interoperability" within the enterprise, or simply new (perhaps bigger) stovepipes? The US DoD Net-centric Data Strategy does not discuss the relationships among COIs. Of course, the DoD enterprise is not divided into separate and distinct COIs, with completely unique languages, as suggested by figure 1.



Figure 1: Distinct COIs

What criteria do we use to determine the logical content and bounds of a COI? Can they be arbitrarily small? When is a COI too big? Or, do they overlap as is suggested by figure 2?

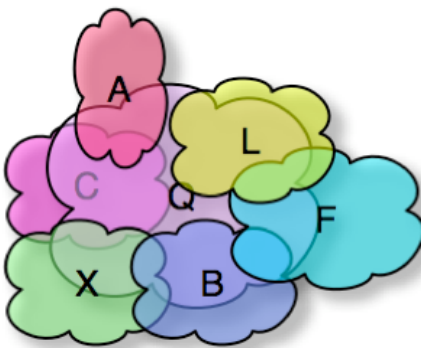


Figure 2: Overlapping COIs

Somehow COIs must overlap in a manner that supports the required mission capabilities. The answer must be driven by the operational requirements of the enterprise! In a phrase, we should consider how "form should follow function". From a DoD enterprise perspective, joint and multinational operations are essential warfighter mission contexts. The United States has said it will work in coalitions and with civil and non-governmental organizations when it undertakes military, anti-terrorism, crisis response and humanitarian operations. The Joint Chiefs of Staff and US Joint Forces Command (JFCOM) are defining Multinational Information Sharing (MNIS) capabilities for working with multinational and coalition partners⁶. The MNIS context is in some respects broader and more difficult than the Joint context⁷. Regardless, multinational operations are appropriate for defining the mission context within which individual communities must work together. Desired MNIS capabilities include[6]:

- Ability to share, collaborate on, or synchronize information with mission partners rapidly and within a net-centric environment. Rapidly access relevant, accurate and timely information in an assured environment and amid unprecedented quantities of operational data to create and share the knowledge required to make decisions with mission partners.
- Ability to interoperate with and leverage mission partners systems. Effectively share information to plan, execute, and monitor the mission and coordinate support for the accomplishment of that mission while adapting to changing situations within an environment containing mission partners.
- Ability to extend US MNIS capabilities to mission partners rapidly and within a net-centric environment. Be aware of and have the ability to integrate and consume disparate C2 and intelligence information from other nations into a cohesive force multiplier in support of the mission or operation objectives.

⁶ Partners are entities, military or civilian, governmental or non-governmental who are participating in a particular mission. Trusted mission partners are defined as member nations that participate with the US in coordinated and cooperative arrangements.

⁷ Information release procedures and information assurance and accreditation complicate multinational architectures and processes.

5. Joint and multinational C2 community of interest

Joint and multinational information sharing capability required by MNIS is to enable effective, coordinated, C2. "Command is the most important function undertaken by a Joint Force Commander (JFC). It is the exercise of authority and direction by a properly designated commander over assigned and attached forces. C2 is the means by which a JFC synchronizes and/or integrates joint force activities in order to achieve unity of command. C2 ties together all the operational functions and tasks, and applies to all levels of war and echelons of command across the range of military operations"[7]. In order to achieve this broad set of operational capabilities, mission area systems and services must appropriately integrate and support the JFC. The commander must be able to exchange information with many subordinate commanders in order to inform, focus and coordinate their actions. Should we require the operational commander to pass the same situational and contextual information to different subordinate commanders using different "languages" because each subordinate is supported by information systems built to different COI interoperability profiles? Should the communications be filtered by translators that reduce the quality of the information sharing?

But wait, commanders are *a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes*. There is a need for a shared command and control COI interoperability profile! Figure 3 shows many types of commanders empowered to work together through a C2 common semantic (language).

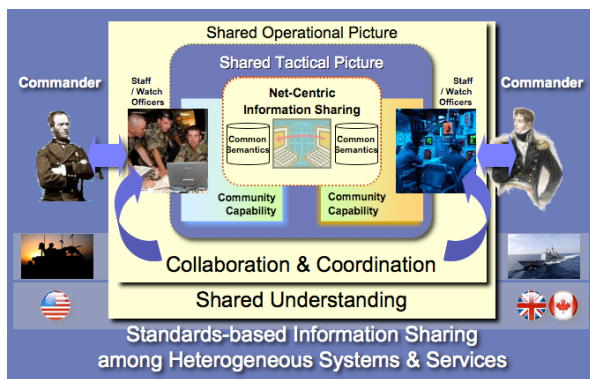


Figure 3. Enabling commanders to work together through standardized data

Figure 3 shows that the C2 COI must obviously include our mission partners. Less obvious, but

equally important, is that the C2 information sharing language used within the US DoD enterprise and among national mission partners must be the same root C2 language. During World War II, General Gavin, Commander 82nd Airborne Division recognized the potential for disaster if the training, terminology, planning documents and map references were not aligned between allies prior to the invasion of the European continent[8]. Since that time US and NATO allies, as well as allies and partners in other regions of the world, have worked to align concepts, language and training. When each nation had its own root C2 language, as with distinct COIs, expensive and imprecise translators are needed when sharing information.

6. C2 common core

A joint and multinational C2 community data standard, a C2 common core, is required to build the next generation of net-centric enabled command capabilities. All non-C2 COIs conceptually and logically overlap this C2 common core to some degree as shown in figure 4. From an operational point of view this is because all warfare communities have a need to exercise some type of command and control internally, and because the actions of all warfare communities must be coordinated, prioritized, de-conflicted, and synchronized with the actions of other partners / warfare communities. This requires high-quality information, rapid sharing and automated processing – which in turn requires that the supporting information systems "understand" the information they receive.

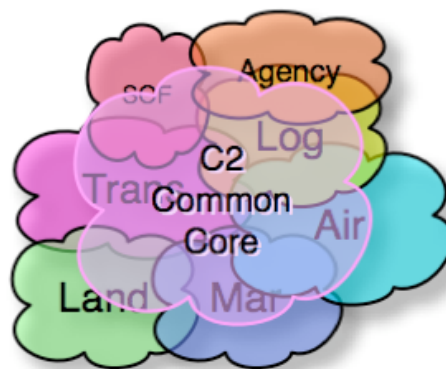


Figure 4. C2 Common Core

Thus, a conceptual and essential foundation for net-centric information sharing is a C2 common core information standard (a shared logical model). When used by other COIs a shared core establishes the necessary initial conditions for understanding shared

information⁸. Community reuse of appropriate portions of a C2 common core builds interoperability through shared language concepts and semantics. A C2 common core can be extended to meet additional COI process and processing needs while retaining the essential conceptual and logical ties to joint C2 processes. Data administration, management, alignment and transformation are key processes that each COI must undertake to normalize, semantically harmonize and simplify information sharing. These processes can exploit a C2 common core[9].

A policy that requires each COI to build on C2 fundamentals reflects the necessary operational / functional requirements prescribed by the warfighter domain. That is, commanders must be able to speak with each other and to their subordinates, regardless of mission specialty. From a technical point of view, there are many concepts that are common across communities, including location, action, things in the battlespace, time, etc., and which are a natural, integral, part of the minimal C2 common core.

What C2 common core standards and related standardization efforts currently exist? There are efforts ongoing motivated by a desire to improve information sharing, planning and coordination. Examples include, legacy military formatted message standards, tactical data link standards, system specific products that have been sold to partners, systems and services under development, Federal agency efforts, and to a limited degree industry efforts. There are also many technical standards that might be leveraged by C2 implementers. These technical standards are enablers but do not address the scope of C2 domain operations or requirements. As an analogy, consider that structural steel, dimensional lumber and engineered lumber all represent available technologies and standards – but the important initial "operational question" is what type of building is required?). There are standardization efforts ongoing in the area of collaboration services, but as currently defined none adequately deal with information content standards and how structured information can enhance collaboration. None of the efforts listed above meet the spirit or technical requirements for a C2 common core. Fortunately, the US (under Army leadership) and

many others have invested in just such a collaborative effort to develop a C2 common core.

7. Multilateral Interoperability Programme



Multilateral Interoperability Programme (MIP) is a premier example of a COI[10]. In a phrase, C2 interoperability and systems integration in a Coalition (and Joint) environment is the MIP *raison d'être*. MIP collaboration and technical work started in the early 1990s. Through a careful and steady process the MIP community has grown and its products have matured. The nations and HQs that are active in the MIP are: Australia, Austria, Belgium, Canada, Czech Republic, Croatia, Denmark, Finland, France, Germany, Greece, Hungary, Italy, Lithuania, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Turkey, United Kingdom, United States, JFC Brunssum and Allied Command Transformation (ACT). MIP is staffed by national warfighter and materiel developer technical teams that meet for two weeks four times per year. The MIP working groups and oversight process produce synchronization time-phased capability and fielding plans and standards. Implementation of the MIP specification is a NATO Force Goal (EL2802).

MIP's conceptual framework and products have evolved over many years, but have always focused on building a common logical representation suited to the commander's critical information requirements. The MIP C2 logical model is the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM).⁹ JC3IEDM leverages past military domain messaging standards, and supports sharing the rich operational context required by Service, Joint and Multinational command and control processes. Its characteristics make it appropriate as a basis for country independent technical standards and products. MIP supports periodic multinational technical, system, and operational testing, evaluation, and demonstration. In 2007, NATO published STANAG 5525 (JC3IEDM), to ensure that national data assets are understandable when made available in a coalition information sharing environment.¹⁰

MIP's accomplishments are impressive and important because it has undertaken arguably the most challenging and critical net-centricity problem — C2 semantic interoperability — in the diverse multinational

⁸ The information system implementers gain "understanding" in the sense that the defined COI interface provides knowledge and removes uncertainty and ambiguity at design / implementation time. This should in turn lead to improved systems and services that contribute to better understanding on the part of the system user. "Understanding" is however something that occurs within a person, thus, shared understanding can not be guaranteed by any technical solution alone.

⁹ The JC3IEDM is a generic, logical, normalized, model that is country, community, process, Service, system, service, technology neutral. The MIP's work is publicly available at www.mip-site.org.

¹⁰ The US ratified STANAG 5525 in 2007.

environment. As a multinational C2 COI, the MIP processes and technical data standards are iconic of the US DoD Net-centric Data Strategy desired result. MIP was honored with the Institute for Defense and Government Advancement (IDGA) seventh annual 2008 Network Centric Warfare (NCW) Award™ for Outstanding NCW Program from a Coalition Partner.

8. Fielding the JC3IEDM C2 common core

JC3IEDM enters service in 2009. For the US, the MIP approach and standards represent a strategic, joint, integration pathway that leads to interoperability with many coalition partners. More than a dozen national and commercial systems are part of a growing set of interoperable allied C2 systems. The US and other nations are preparing to field their current generation of MIP compliant systems in Afghanistan. NATO and nations are applying MIP data standards as a basis for force management, warfare operations, crisis response, stability operations applications, modeling and simulation, information sharing, and supporting services. The MIP COI process and standards work are on the upswing and provide a new and critical foundation for Service, Joint, and Coalition information sharing interoperability in the emerging net-centric warfare environment. Examples of MIP influence on US system and related net-centric activities include:

- US JFCOM, J87, supporting the C2 Capability Portfolio Management process, working with Service and community representatives, defined an initial joint US C2 Core Data Model. The initial US C2 Core, published at the beginning of April 08, is based on the JC3IEDM. It leverages and exposes about 1/3 of the JC3IEDM's total elements - (C2).¹³
- Global Force Management COI is producing a DoD enterprise set of data services that uses JC3IEDM to provide force management data on all Joint assets (people, equipment, organizations) - (GFM).¹³
- The U.S. Army data strategy and acquisition policy are to implement JC3IEDM. Maneuver Control System 6.4 is MIP compliant, Future Combat System is leveraging MIP data standards, and the Army's Net-centric Center of Excellence is building a JC3IEDM Service Oriented Architecture (SOA) pilot. The Army has also developed a beta software development kit (SDK)

which is being used to support the SOA pilot and other projects.

- DISA has conducted C2 services prototyping using C2IEDM (the JC3IEDM pre-cursor) - (NEC2IEDM).¹³
- The U.S. Marine Corps has recognized the operational utility of the JC3IEDM and made it a core part of the USMC data strategy.¹⁴
- The Navy has conducted at-sea experiments and shown the utility (i.e., lower bandwidth, decreased time, improved understanding) of using the JC3IEDM to build improved collaborative work environments.
- Coalition Secure Management and Operations System (COSMOS), a multinational (USA, GBR, CAN, AUS, SGP) US Advanced Concept Technology Demonstration (ACTD), has partnered with National Security Agency and uses the C2IEDM and JC3IEDM strong data semantics to create a mixed information management and information assurance foundation for protected information sharing with allies.¹⁵
- JC3IEDM is being submitted to the Object Management Group C4I Domain Task Force in response to the Shared Operational Picture Exchange Services (SOPES) request for proposals.¹⁶
- To better integrate C2 and modeling and simulation type systems the Simulation Interoperability Standards Organization (SISO) and NATO Research Technology Organization (MSG-48) are conducting coordinated standardization efforts using JC3IEDM.¹⁷
- The multinational CBRNE COI data model is based on and extends the JC3IEDM - (CBRN).¹³

9. Summary

During joint and multinational operations commanders and decision makers need to plan, inform, coordinate, allocate, de-conflict, and synchronize effort. The power of net-centricity is measured in terms of the number of nodes and the degree to which they are able to effectively share information. Many small isolated domains coupled by translation will lead to weak integration and limited

¹³ See: <https://metadata.dod.mil/mdr/and>
Namespace=C2, Namespace=GFM,
Namespace=NEC2IEDM, or Namespace=CBRN

¹⁴ [http://www.marines.mil/news/messages/Pages/MARADMIN Number: 044/08](http://www.marines.mil/news/messages/Pages/MARADMIN%20Number%20044008)

¹⁵ Joint Capability Technology Demonstration Transition
Funding PE 0604648D8Z

¹⁶ <http://www.omg.org/cgi-bin/doc?c4i/2004-6-27>

¹⁷ [http://www.sisostds.org/SISO Groups, Product
Development Groups, Coalition Battle Management
Language \(CBML\)](http://www.sisostds.org/SISO%20Groups,Product%20Development%20Groups,Coalition%20Battle%20Management%20Language%20(CBML))

shared understanding. Achieving the net-centric desired operational capabilities to quickly, accurately and unambiguously coordinate operations depends on establishing a strong, ubiquitous, semantically rich, extensible C2 common core language.

This strategy prioritizes COI standards, promoting the C2 common core, to achieve operational and technical integration. That core forms the foundation for essential and ubiquitous warfighter business processes. It imposes on the technical and acquisition communities necessary enterprise operational constraints. This holistic perspective may seem overblown and unnecessary to those working the details of a given system or service. Regardless, C2 common semantics are required as the enabling framework to achieve the net-centric power envisioned and needed.

10. Recommendations

DoD leadership continue to:

- Support the Joint C2 Capability Portfolio Management (C2 CPM) process and its expressed interest in a US C2 common core.
- Ensure that Joint C2 CPM focuses on the essential operational requirements for conducting joint and multinational operations and establishes data standards with commensurate scope.
- Ensure that C2 governance requires mandatory reuse of the logical C2 common core (US C2 Core) by functional COIs, where information sharing between COIs is needed. Reuse should be assessed and evaluated by a C2 common core advocate.
- Ensure that COI languages are consistent with the logical C2 common core. Ensure that extensions outside of C2 are harmonized with other interested COI.
- Build-up and sustain a joint workforce with the required analysis and modeling skills to support the development of the objective net-centric information sharing environment.
- Improve as required, and expand the use of, the JC3IEDM as the baseline for the US C2 Core. Support JC3IEDM continued maturation and promotion in the multinational community. Enhance US joint participation in the MIP community.
- Promote the adoption of the C2 common core by sponsoring prototyping and experimentation efforts and designation of early adopter / implementer programs.
- Assist functional community COIs to adopt and extend the C2 common core with analysis, training and modeling activities.

11. References

- [1] DOD Net-Centric Data Strategy, DOD Chief Information Officer, 9 May 2003
- [2] Alberts, David S. 2007. *Agility, Focus, and Convergence: The Future of Command and Control*. Washington: CCRP
- [3] Col Kevin Jordan, USMC, US Pacific Command, J63, Camp HM Smith, Hawaii, COSMOS ACTD Operational Problem Description. Jan 2005.
- [4] COL Stuart Whitehead, USA, Military Review, *Battle Command, Toppling the Tower of Babel*, September-October 2005.
- [5] DoD Information Sharing Strategy, DOD Chief Information Officer Memorandum, 4 May 2007.
- [6] Initial Capabilities Document (ICD) for Multinational Information Sharing (MNIS), 30 August 2007
- [7] Joint Publication 1, *Doctrine for the Armed Forces of the United States*. 14 May 2007
- [8] Gavin, James M. 1978. *On to Berlin: Battles of an Airborne Commander 1943-1941*. The Viking Press, New York
- [9] Tolk, Andreas. Sailou Y. Diallo. July-August 2005. *Model-based Data Engineering for Web Services*. IEEE Internet Computing
- [10] Multilateral Interoperability Programme web site. www.mip-site.org

Authors:



Mr. Richard P. Lee

Mr. Lee is the Assistant Deputy Under Secretary of Defense for Information Integration and Operations, Office of the Under Secretary of Defense (Acquisition, Technology & Logistics), Defense Research & Engineering Directorate, Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, with oversight for Advanced Concepts and Joint Capabilities Technology Demonstrations in communications, information operations, interoperability, and computer network defense. Mr. Lee served in the United States Navy as a Surface Warfare Officer, commanding *USS OLIVER HAZARD PERRY (FFG 7)* from 1990 to 1992. Ashore he served as a Military Observer with the United Nations, managed various communications, command and control, and information operations programs. He retired as a Captain in 1999. Mr. Lee joined the Office of the Secretary of Defense in May 2001. He is a graduate of the US Naval Academy with a Bachelor of Marine Engineering degree, and holds a Master of Electrical Engineering degree with a concentration in communications systems from the US Naval Postgraduate School.



Mr. Erik Chaum

Mr. Chaum is a member of the Center for Advanced System Technology at the Naval Undersea Warfare Center, Newport, RI. He performs command and control research, experimentation and standardization work in multiple multinational fora including; the Multilateral Interoperability Programme (MIP) as a member of the U.S. delegation, and The Technical Cooperation Program (TTCP) where he is the U.S. National Leader in Maritime Systems Group's Maritime Command and Control and Information Management Panel. In the recent past he served two years as the Assistant Director, Defense Modeling and Simulation (M&S) Office focused on M&S and C2 interoperability. In this capacity, he additionally served as a M&S TTCP National Leader and NATO RTO co-chair. He has led Navy C2 experimental initiatives looking at innovative techniques to improve man-man and man-machine collaboration through sharing JC3IEDM structured data. Mr. Chaum is a 1977 graduate of the US Naval Academy and a 1984 graduate from the Massachusetts Institute of Technology (MIT) Management of Technology program.



Command and Control Common Semantic Core Required to Enable Net-centric Operations

AFCEA–George Mason University:
Critical Issues in C4I

Mr. Erik Chaum
Naval Undersea Warfare Center
(401) 832-6915
ChaumE@npt.NUWC.Navy.mil

Mr. Richard Lee
DDR&E (Advanced Systems & Concepts)
(703) 695-7938
Richard.Lee@OSD.mil

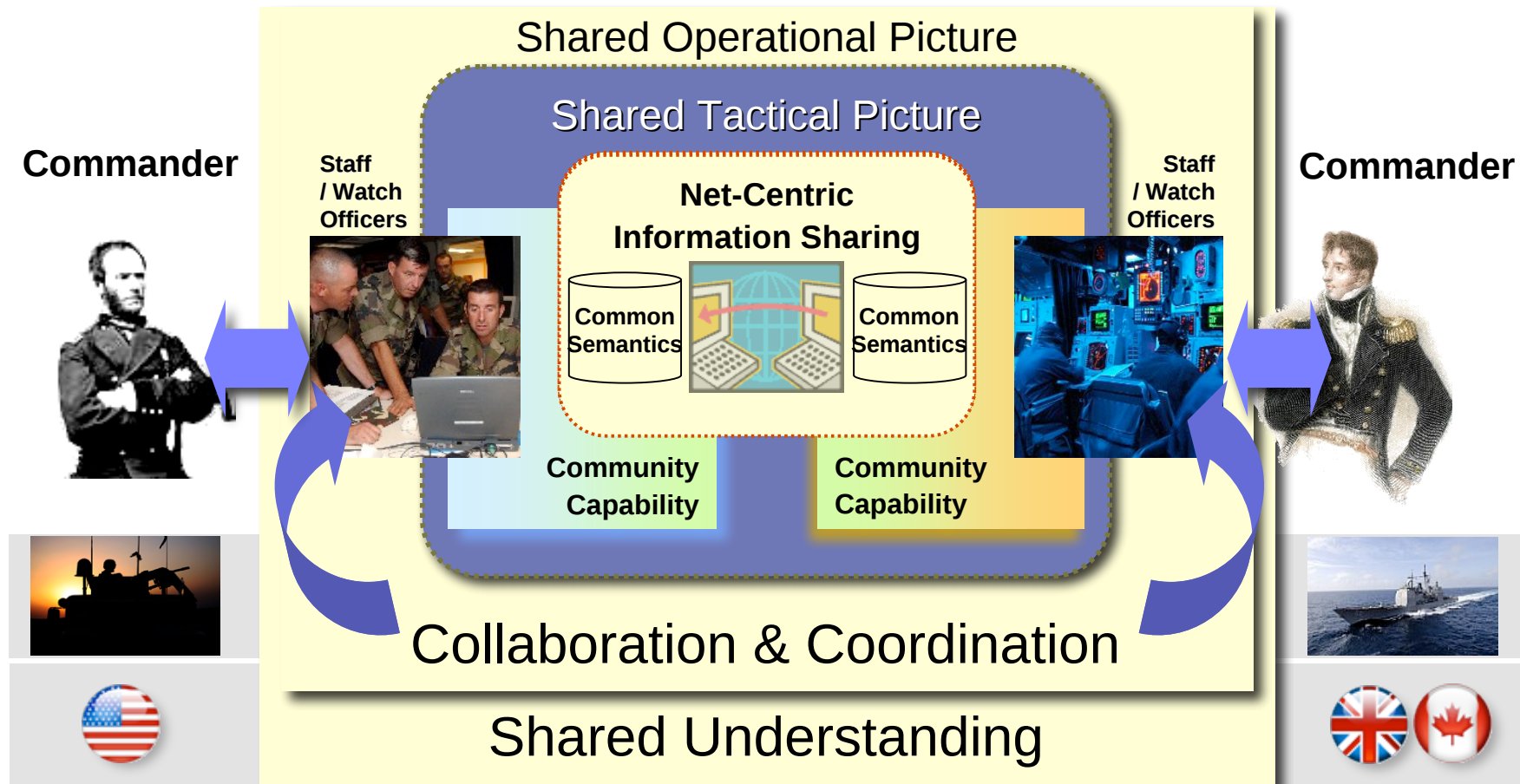


Understanding Shared Information

- Commanders and other decision makers require timely and accurate information
 - the power of information, and information sharing, are fundamental tenets of the ongoing defense transformation
 - we lack a shared precise language!
- Transformation guidance - make information:
 - visible,  Straight forward - Commercial technology
 - accessible, and  Straight forward - Commercial technology
 - understandable  Difficult - Military/Joint domain knowledge



Information Sharing & Shared Understanding



**Objective: Standards-based Information Sharing
among Heterogeneous Communities, Systems & Services**



As Is

- "Tower of Babel" - point-to-point information sharing capabilities:
 - unique interface languages for specific systems
 - expensive to build and maintain
 - in the net-centric context, provides relatively limited information sharing or automated processing capability
- Community and system-specific models are seldom equivalent, resulting in limited sharing and shared understanding:
 - translation (a.k.a., mediation) is necessary to access legacy data
 - translation can result in loss of precision, meaning, and or context
- Translation can inject uncertainty and ambiguity degrading the quality of information being shared
 - these losses are typically not shared with the decision maker!
- Maintaining the quality and context of information as it is being shared is critical to it being properly understood and subsequently used by the decision maker.



Shared Language

- Can flatten, broaden and speed information sharing:
 - between people,
 - between information systems[†], and
 - between people and information systems
- Important when people share information:
 - knowledge of the "language" and "business" process are key
 - we rely on his / her training and knowledge to process information
 - search engines, web page technology have enabled a revolution in discovery and access but mostly continue to rely on manual user interpretation
- Net-centric operations require much more than discover and display. We must be able to:
 - share information among many types of systems and services
 - reliably process shared information in an automated manner

[†] Information systems: any type of networked software-based system, application or service.



Synchronized Effort Needed

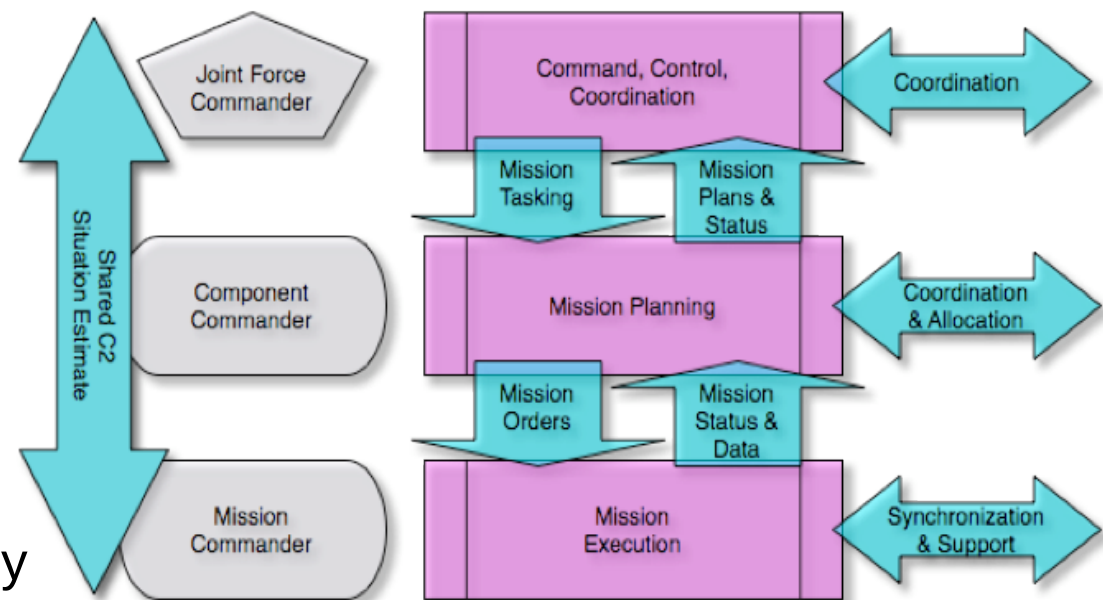
- The US DoD Net-centric Data Strategy (NCDS) begins to address this problem with the establishment of Communities of Interest (COI), a:
 - "collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange"
 - necessary but not sufficient!
- The DoD Information Sharing Strategy[†] notes:
 - that there have been "numerous independent mission or functional area specific initiatives addressing aspects of information sharing" and says
 - **"these strategies and efforts must be synchronized in order to achieve unity of effort as well as economic and operational efficiencies"**
 - What is the appropriate synchronization baseline?
- Integrated capability is the objective:
 - Corollary: No single organization, system or service provides an end-to-end operational mission capability
 - each community works with many others to achieve effects and objectives
 - Joint C2 process and language form the baseline for net-centric operations and information sharing

[†] 04 May 2007



Integrated Capability

- C2 information flows among and between:
 - operational commander,
 - supporting functional area commanders, and
 - mission commanders.
- Information must be understood and flow :
 - Vertically and horizontally
 - SA used at all levels

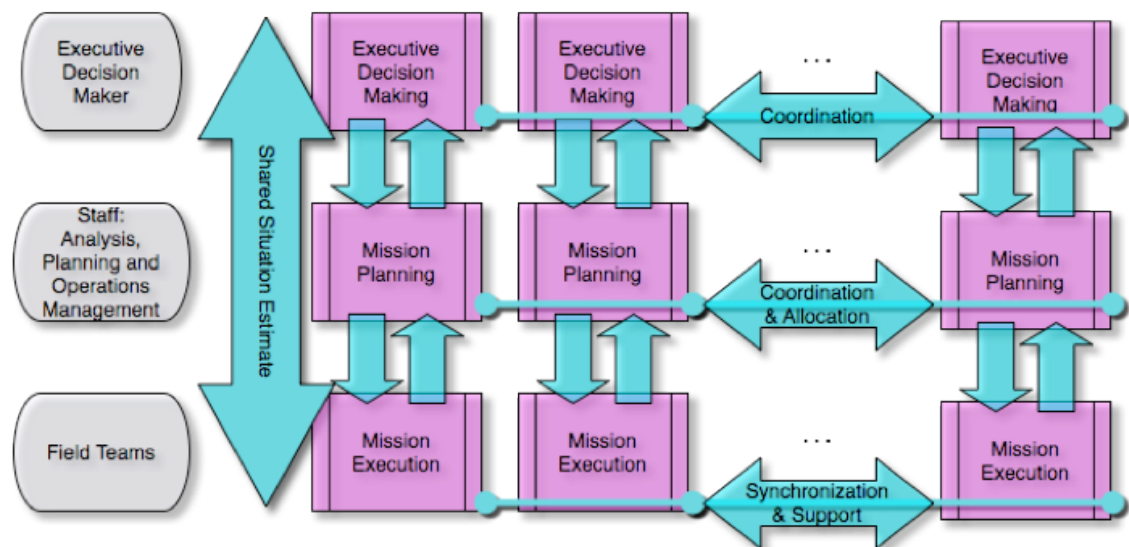


This conceptual model
is joint, but applies equally
well in any functional community.



Integrated Capability [2]

- CJTF, StabOps, inter-agency context and associated information flows among and between:
 - executive decision makers,
 - organizational staffs, and
 - field teams.
- Alt, a vertical stack is a separate joint component commander and the supporting information flows and activities.
- Complex operations, a blend of:
 - traditional C2 and
 - horizontal collaboration
- Expanding the quality and scope of standard (normalized and harmonized) C2 data will enable, simplify and improved processes and information processing.

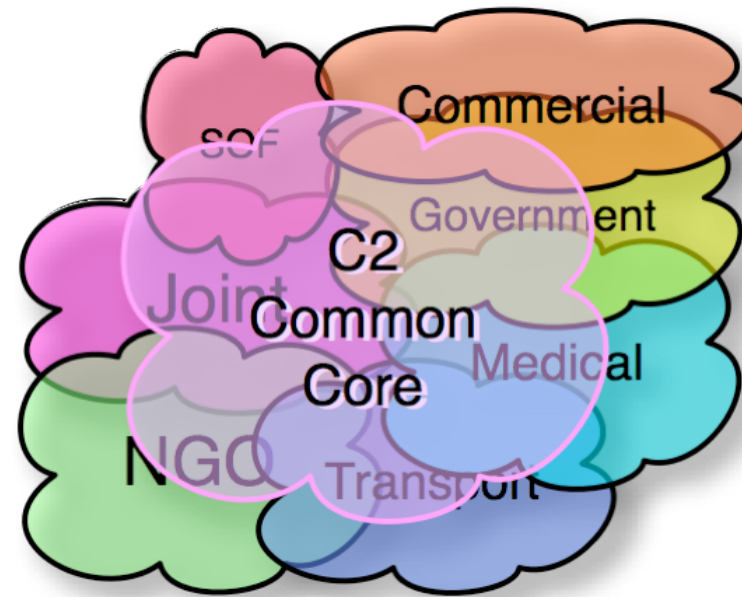


Joint and Combined -
common patterns, processes
and information sharing needs



An Enabling Constraint

- Community languages are unique, but, overlap!
- In an operational context each community must share information with others.
- All communities use concepts and semantics familiar to C2.
- C2 and collaboration are critical business processes for all.
- An essential **enabling constraint** is a widely understood normalized and harmonized C2 core language - a simplified logical language empowering communities to work together.



Each "cloud" conceptually represents a community language.



Information Baseline

- The scope of C2 information / language includes basic current situation estimates and contextual knowledge about:
 - battlespace objects
 - objectives
 - operational and tactical plans (e.g., orders, status, forces, capabilities, control measures, rules of engagement, logistics, etc.)
 - situation estimates
 - natural and cultural environmental knowledge
- Normalizing C2 information at the joint / coalition level:
 - simplifies its sharing, understanding and improves processing, analysis & fusion
 - enables improved business processes and processing
 - helps ensure that enterprise and mission software / services are able to "understand" a broader set of relevant information and thus provide better informed recommendations and capabilities
 - enables migration to Joint standardization
 - IAW CJCSI 5705.10c (Joint Terminology) and JP 1-02
 - provides a baseline formal language for addressing UJTLs, etc.



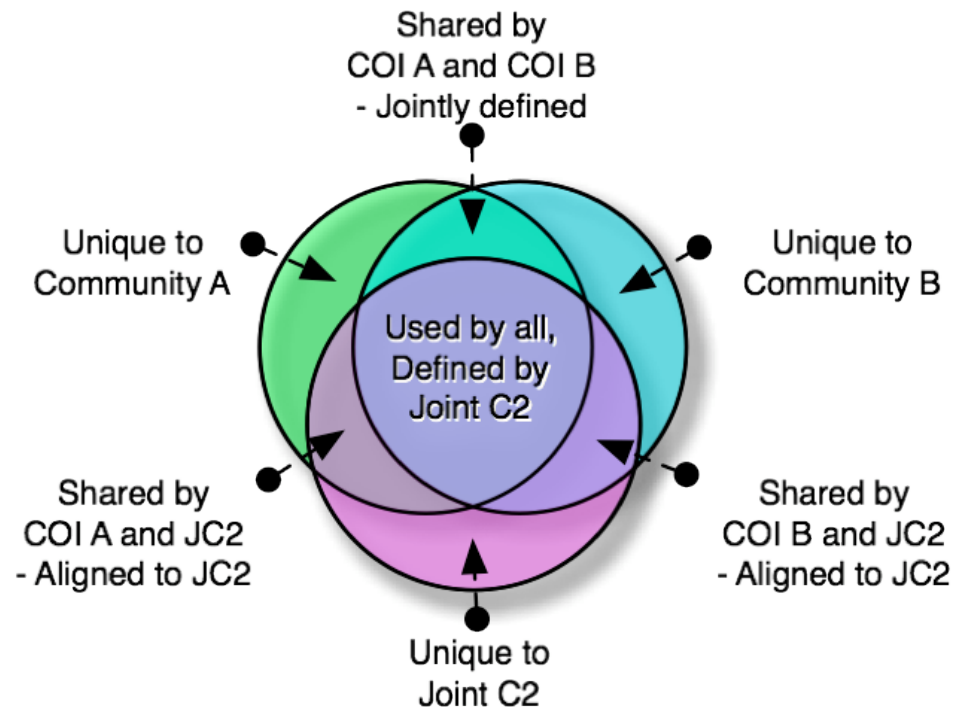
Net-centric “To Be”

- A lean collection of systems and services that "plug-and-play":
 - add value at the joint / operational level
 - add value to warfighter-defined community processes
 - loosely coupled - architecturally
 - strongly coupled - semantically, shared domain languages
 - follow prescribed business rules
- A well-defined COI interoperability profile defines:
 - for legacy systems how they must evolve
 - creates for new systems and services a clean community design baseline
 - normalizes to, and harmonizes with, joint interfaces
- Open architecture supporting horizontal and vertical integration
 - governance or funding must support
 - must be embraced by Services and partners



Cornerstone: Joint C2

- Overlaps are where:
 - semantic differences create understanding gaps
 - harmonization and standardization are essential,
 - too often we see duplication and fail to capture operational and economic efficiencies, and
 - programmatic and governance issues must be addressed.
- We need rationale and criteria to resolve how to organize and reengineer in the overlaps.
 - C2 is the essential process
 - **Joint C2 operational requirements set the essential criteria for standardization and integration decisions in the overlap!**



Normalized, Harmonized
and Aligned COI
Information Sharing

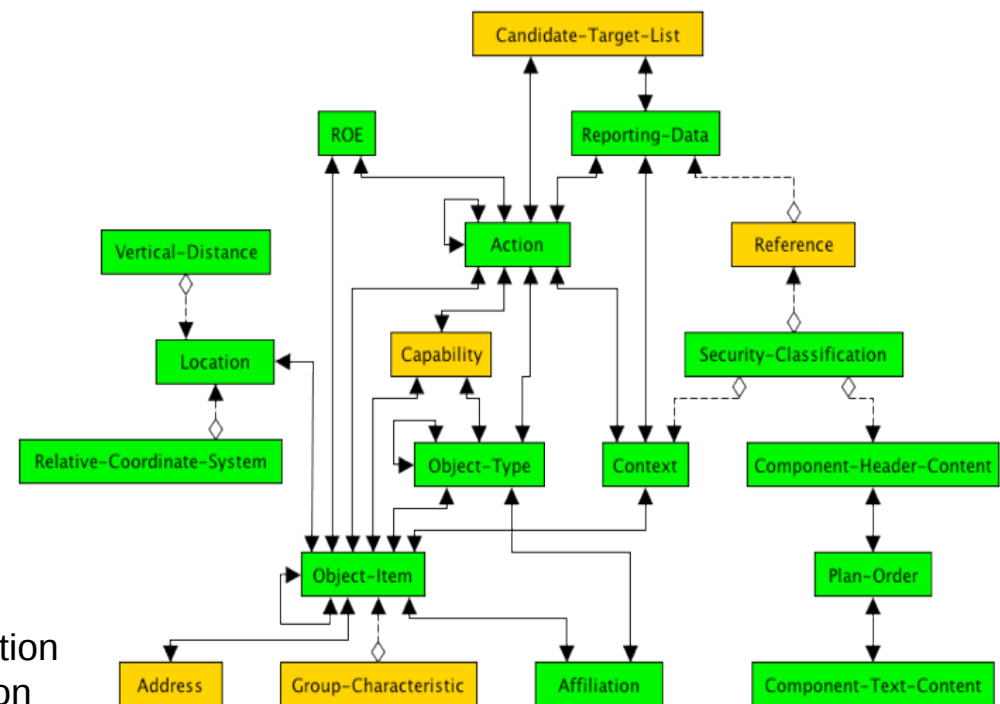


Joint / Multinational C2 Core

- Multilateral Interoperability Programme (MIP)
 - COI: 26 Nations, NATO, ACT
- Operational Objective: Enable common understanding of the battlespace
- Technical Objective:

“Information interoperability” that can:

 - Span national and language boundaries
 - Span echelons
 - Bridge diverse organizations and agencies
- Product: Logical Data Model - JC3IEDM
 - Joint Consultation, Command and Control Information Exchange Data Model
 - Full documentation at: www.MIP-site.org
- Use - C2 Interoperability Standard:
 - System/service interface exchange specification
 - Joint / Coalition normalization & harmonization
- USJFCOM (J8) & OASD NII (C2 Policy) oversee the C2 Capability Portfolio Management Process
 - US Joint C2 core data exchange model for joint, multinational, and StabOps information
 - Leveraging the JC3IEDM



■ US C2 Core (v1)

■ + ■ JC3IEDM





Some US JC3-related Efforts

- US C2 Core: US JFCOM, J87 & OASD NII C2 Policy led C2 Capability Portfolio Management process. Define a joint US C2 Core Data Model. Initial version based on JC3IEDM (April 08).
- Global Force Management: DoD enterprise data services to provide force management data on all Joint assets (people, equipment, organizations).
- U.S. Army data strategy and acquisition policy are to implement JC3IEDM. Aligned: MCS, FCS, and JC3IEDM Service Oriented Architecture (SOA) pilot.
- The U.S. Marine Corps has recognized the operational utility of the JC3IEDM and made it a core part of the USMC data strategy.
- JC3IEDM-enabled collaboration: Navy at-sea experiments showed the utility (i.e., lower bandwidth, decreased time, improved understanding) of collaborative work environments using JC3IEDM.
- ACTD: Coalition Secure Management and Operations System (COSMOS), a multinational (USA, GBR, CAN, AUS, SGP) Advanced Concept Technology Demonstration. Partnered with National Security Agency and uses the C2IEDM and JC3IEDM strong data semantics to create a mixed information management and information assurance foundation for protected information sharing with allies.
- Object Management Group C4I Domain Task Force: Proposal to use JC3IEDM as baseline for Shared Operational Picture Exchange Services (SOPES) .
- C2 and modeling and simulation: Simulation Interoperability Standards Organization (SISO) and NATO Research Technology Organization (MSG-48) are conducting coordinated standardization efforts using JC3IEDM.
- Multinational CBRNE: COI data model is based on and extends the JC3IEDM - (CBRN).



Conclusion

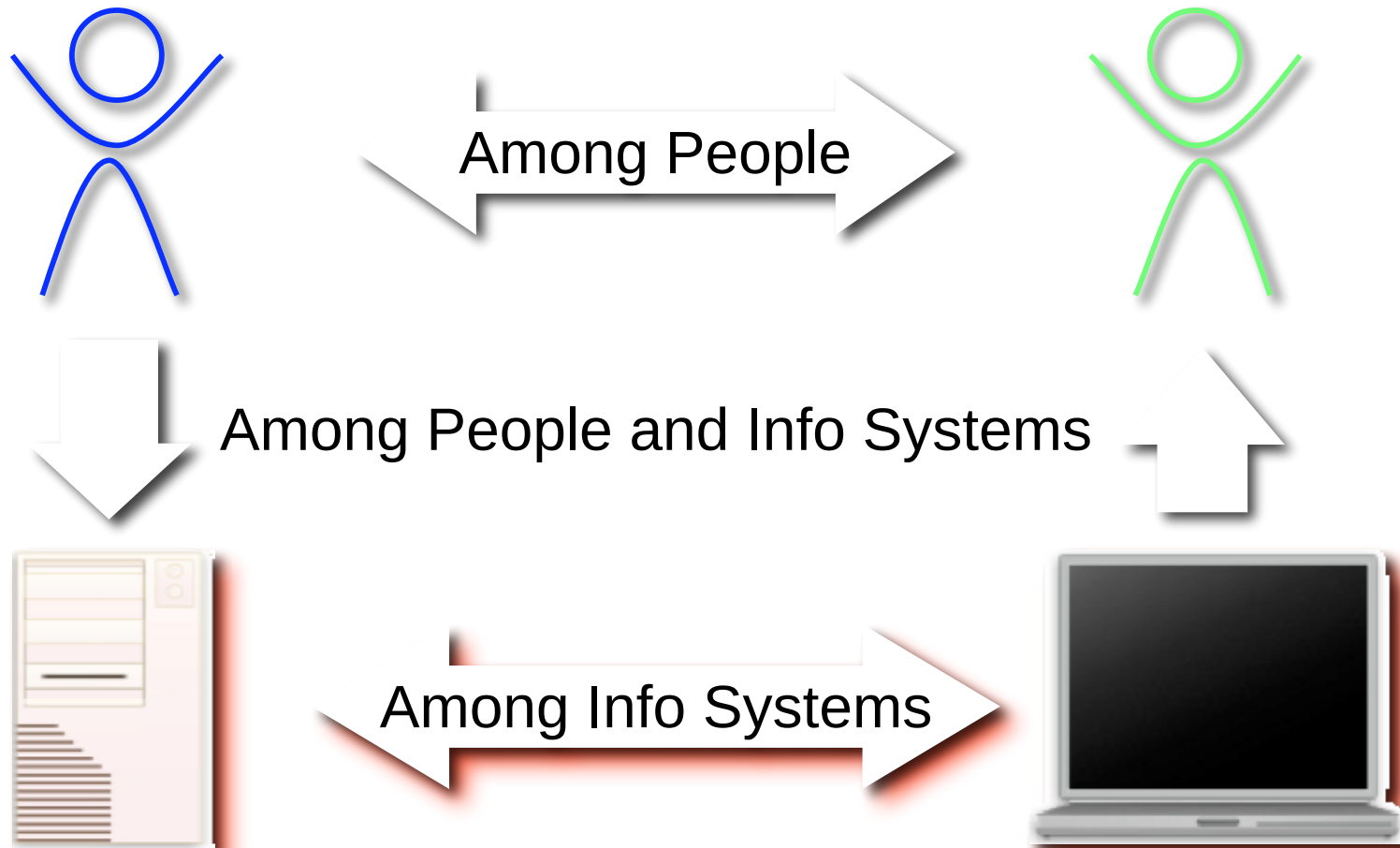
- Military decision makers and systems need a common C2 language to:
 - ensure information shared is understood
 - enable more automated sharing and processing, and
 - enhance and simplify essential military processes (e.g., alerting, planning, coordination, de-confliction, and synchronization)
- A Joint and multinational-level C2 language provide the proper level of abstraction and integration for net-centric operations:
 - enables the appropriate enterprise / operational information flows
 - can be leveraged and extended to meet Service and mission-specific information sharing needs, retaining the necessary link to joint
 - provides an enabling constraint that moves us away from imprecise translation and legacy point-point interfaces between systems
- A shared C2 core foundation is essential for net-centric warfighter processes
 - It imposes on the technical and acquisition communities necessary enterprise operational requirements and constraints
 - Leverage the existent multinational C2 data standards, specifically JC3IEDM
- Reengineering and transformation require suitable governance & funding



Back-up



Types of Information Sharing



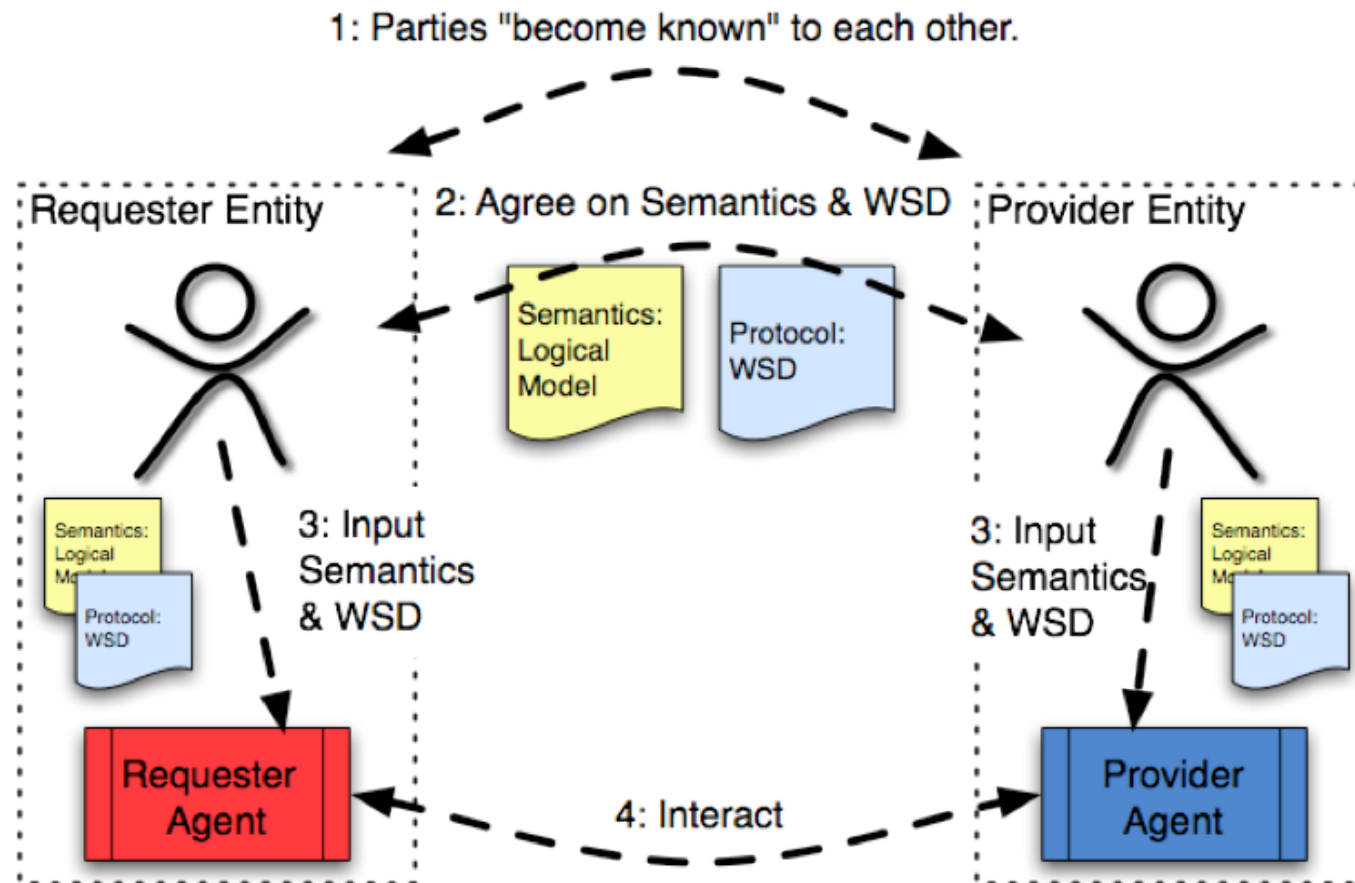


Better Informed - Better Able

- Better informed warfighters are able to operate with increased confidence and agility in a more timely, and synchronized manner
 - better informed information systems provide the higher value services required in more demanding operational scenarios and processes
- Collaboration is likely to be more successful and efficient when the participants have a common understanding of the shared information
 - i.e., they working to decide what to do, not spending time trying to resolve discrepancies in their interpretations of the shared information



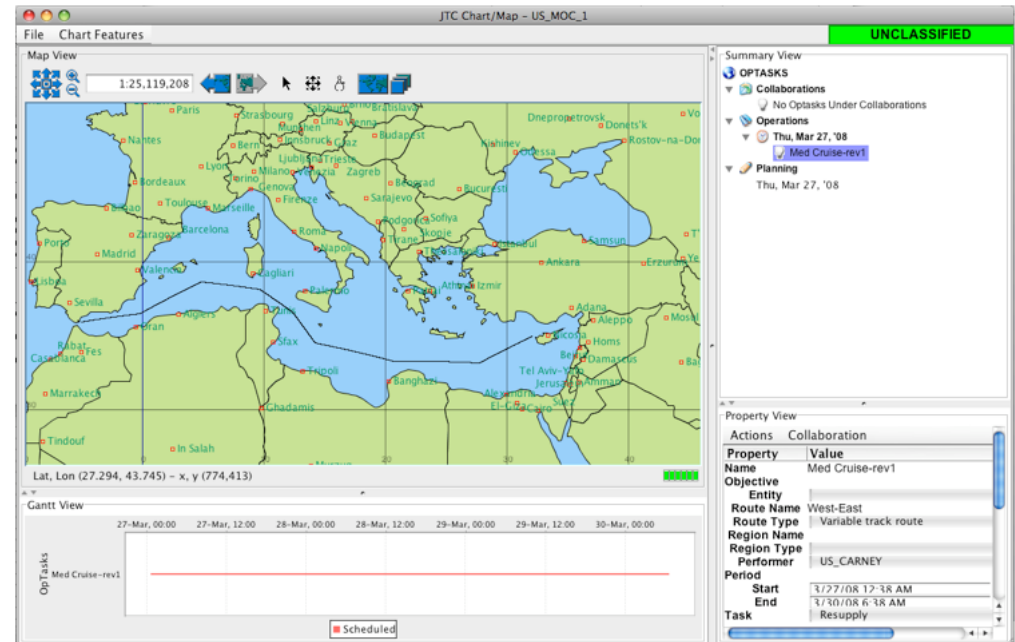
“Everything should be as simple as it is, but not simpler.” [Albert Einstein]





Enabling Collaboration

- "The networking of knowledgeable entities enables them to share information and collaborate to develop shared awareness, and also to collaborate with one another to achieve a degree of self-synchronization". [Alberts, Garska, Stein 1999]
 - *focus and convergence* - new high abstract concepts. [Alberts 2007]
 - understanding shared information is essential. It:
 - can empower the decision makers to operate in a more agile, timely, and synchronized manner
 - emphasizes teamwork in the heterogeneous StabOps environment.



JC3IEDM-enabled CWE

- Collaborative work environments (CWE) enhance the performance of common command and control activities:
 - create commonly-alterable work products / information objects—such as plans, orders, graphics, analyses, estimates
 - support decision makers in the comparison and assessment of shared plans, visualizations, work products or other information objects in order to reach mutual understanding.



References

- [1] Multilateral Interoperability Programme (MIP) www.MIP-site.org
- [2] DOD Net-Centric Data Strategy, DOD Chief Information Officer, 9 May 2003
- [3] DoDD 8320.02 - Data Sharing in a Net-Centric Department of Defense, 2 Dec 2004
- [4] Command and Control Information Exchange Data Model, US Army DCS G-3/5/7 DAMO-SBB Memorandum, 28 Feb 2005
- [5] JPEO-CBD CBRN Data Model Overview, S. Vachher, Dr. T. Johnson, 14 Nov 14, 2006
- [6] DoD Information Sharing Strategy, DOD Chief Information Officer Memorandum, 4 May 2007
- [7] CJCSI 5705.01C Joint Terminology, 19 Feb 2008
- [8] Global Force Management Data Initiative Implementation Plan (GFM DI I-plan), Chairman, Joint Chiefs of Staff Force Structure, Resources, and Assessment Directorate (J-8) February 5, 2007
- [9] Joint Publication 1, *Doctrine for the Armed Forces of the United States*. 14 May 2007
- [10] Alberts, David S. 2007. *Agility, Focus, and Convergence: The Future of Command and Control*. Washington: CCRP
- [11] Initial Capabilities Document (ICD) for Multinational Information Sharing (MNIS), 30 August 2007
- [12] Simulation Interoperability Standards Organization, Coalition Battle Management Language (CBML), Product Development Group, www.sisostds.org topic CBML
- [13] US Marine Corps Information Exchange Policy, MARADMIN 044/08, 16 Jan 2008