13th ICCRTS: C2 for Complex Endeavors

Paper 168

"Making Stability Operations Less Complex While Improving Interoperability"

C2 Concepts, Theory, Policy

Multinational Endeavors

Civil Military Endeavors

by

Erik Chaum, Gerard Christman

Point of Contact: Gerard Christman

Name of Organization: OASD(NII)

6000 Defense Pentagon Room 3E173

Washington DC 20301

(703) 697-8195

Gerard.christman.ctr@osd.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Making Stability Operations Less Complex While Improving Interoperability	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) **OASD(NII),6000 Defense Pentagon Room 3E173,Washington,DC,20301**	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
13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT
Military support for stability, security, transition, and reconstruction as well as humanitarian assistance / disaster relief operations is as important and complex an endeavor as is major combat operations. A strategy will be presented, in keeping with US Department of Defense Network Centric Data Sharing policies, to make information sharing during stabilization operations less complex and more effective. This paper exposes how the emerging Stability Operations community of interest can leverage an open standard semantic core for multination command and control information sharing and how it provides an essential, extensible, foundation for communication among international organizations, non-governmental organizations and the military during stability operations. The vision, strategy, and methodology for diminishing complexity and increasing interoperability are presented.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**40**	

Paper 168

"Making Stability Operations Less Complex While Improving Interoperability"

Mr. Erik Chaum
Naval Undersea Warfare Center
ChaumE@npt.nuwc.navy.mil

Mr. Gerry Christman
OASD NII (IICT)
Gerard.christman.ctr@osd.mil

Abstract

Military support for stability, security, transition, and reconstruction as well as humanitarian assistance / disaster relief operations is as important and complex an endeavor as is major combat operations. A strategy will be presented, in keeping with US Department of Defense Network Centric Data Sharing policies, to make information sharing during stabilization operations less complex and more effective. This paper exposes how the emerging Stability Operations community of interest can leverage an open standard semantic core for multination command and control information sharing and how it provides an essential, extensible, foundation for communication among international organizations, non-governmental organizations, and the military during stability operations. The vision, strategy, and methodology for diminishing complexity and increasing interoperability are presented.

Keywords: stability operations, community of interest, data strategy, C2 semantic core, JC3IEDM, US DoD Directive 3000.05, US DoD Directive 8320.02

Stability Operations

Today's warfighters are likely to find themselves immersed in stability, security, transition, and reconstruction (SSTR[1]), humanitarian assistance or disaster relief operations (collectively referred to as stability operations - StabOps[2]). These operations are every bit as important and complex as are major combat operations. There is need to improve warfighter processes and capabilities in these areas in a manner that addresses the inherent real-world complexity while enabling better interoperability within the military, with other US agencies, with other nations, and with non-governmental organizations. StabOps partnerships rely on managed information sharing, collaboration, shared planning, alerting, and coordination. The same can be said for command and control (C2) processes and information sharing. The challenge therefore is to recognize that StabOps must seamlessly integrate with, and support, traditional military operations. In turn this knowledge provides useful conceptual and technical opportunities, guidelines and constraints. This paper addresses how a StabOps community can build and benefit, operationally and technically, from alignment with, and reuse of, multinational C2 information sharing standards.

[1] Military support to Stability, Security, Transition and Reconstruction (SSTR). Department of Defense activities that support U.S. Government plans for stabilization, security, reconstruction and transition operations, which lead to sustainable peace while advancing U.S. interests.

[2] Stability Operations. Military and civilian activities conducted across the spectrum from peace to conflict to establish or maintain order in States and regions.

Following DoD directives, a Stability Operations community of interest (COI) is being established to provide liaison and to help build the operational and technical consensus required to guide StabOps activities and acquisition. Specifically, it is to arrive at a complete, yet succinct standard taxonomy and methodology for extranet information sharing in the COI. New, open, multinational C2 information sharing standards provide an essential, extensible, interoperability baseline for exchange among heterogeneous C2 type services and systems. This paper addresses how C2 data standards can provide immediate benefits including simplified net-centric C2 solutions engineering and improved operational interoperability.

Complex Endeavors

"StabOps are a core U.S. military mission that the Department of Defense shall be prepared to conduct and support. They shall be given priority comparable to combat operations and be explicitly addressed and integrated across all DoD activities including doctrine, organizations, training, education, exercises, materiel, leadership, personnel, facilities, and planning."[3] "Stability operations are conducted to help establish order that advances U.S. interests and values. The immediate goal often is to provide the local populace with security, restore essential services, and meet humanitarian needs. The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society."[4]

StabOps are inherently complex for many reasons including the scale and scope of operations, the variety and interdependence of objectives, the professional and cultural diversity of participants, the types of organizational relationships among participants, the required levels of trust and associated security concerns, operations tempo and often associated time-critical demands on decision makers. Additional complexity arises from environmental factors (e.g., season, region), the wide range of techniques and technologies for information sharing and doctrinal differences in how we choose to organize, coordinate, and synchronize operations. An awareness of the many facets that make StabOps complex leads to an appreciation that technology alone will not provide satisfactory solutions. Rather, capabilities must be shaped by a deep understanding of the operational domain and the needs of the user.

The richness, complexity, criticality, and human nature of such collaborative endeavors does not precludes simple improvements but it does make more holistic process improvements difficult. Being able to establish effective efficient StabOps processes among many diverse participants (i.e., within an organization) and partners (i.e., among organizations) is difficult but essential. The United States, for political and other reasons, will continue to choose to work in coalitions and with civil and non-governmental organizations when it undertakes StabOps operation. The US will also choose to enable and empower Non Governmental Organizations (NGOs), International Organizations (IOs) and civil authorities to perform the functions they were designed to accomplish so that the US Regional Combatant Commands do not have to bear the burden on

[3] DoD Directive 3000.05

[4] ibid

their own. Alberts[5] has examined the suitability of traditional command and control concepts and terminology and argues that fundamental changes are required to effectively perform in coalition combat and StabOps. While there are multiple rationales, an argument made is that the coalition and StabOps environments are complex "comprised of a set of heterogeneous entities including both military and civil government organizations as well as international and private ones, . . not amenable to unity of command or a traditional hierarchy organized around strategic, operational and tactical levels. Such a coalition (is) unlikely to possess the unity of purpose and discipline that are assumed to be present in a military organization." While StabOps are admittedly likely to be more loosely organized and coordinated, there remains a need for partners to establish collaboration processes and to effectively manage and understand information exchange in the pursuit of individual and shared goals.

Sharing Information

The strategic value of information is well appreciated today. So are the multiplier effects when that information is appropriately shared in a timely manner, or potential negative consequences when withheld. There are many prerequisites to effective communications and interoperability. Sharing information itself is a complex endeavor and typically might incorporate many assumptions about the sharing context and the recipient. Communications is never context free, there are always aspects of community, culture, cognitive skills and technology evident. Accordingly, educational, cultural and technological factors can both enable and hinder information sharing, shared understanding and achieving interoperability. This in turn means, not surprisingly, that it is easier to work well with others that share the same training, culture, and tools. Information sharing contexts include:

- Sharing among people: Information is conveyed between people using language and non-verbal behaviors. Within a community understanding shared information is easier because of shared perspective and knowledge achieved through common training and experience. Conversely, novice community members, or members of other communities, may not intuitively understand community concepts, processes, signals or semantics (e.g., vocabularies).
- Sharing between people and information systems (of all types): Information is conveyed through a user interface. Ideally this interface has been optimized for community-specific information and tasks. It is worth noting that independent of community, there are common concepts and presentation patterns (e.g., location; maps, collections; lists, time-ordered; timelines) that can be reused and specialized.
- Sharing among information systems: Information sharing among systems is accomplished through interfaces with well-defined protocols, business rules and semantics (e.g., WSDL, SOAP and XML payloads for community information objects). Information sharing between independently developed systems, or functional community standards, will likely require semantic (and syntactic) translation. Semantic translation is almost always lossy, losing some aspect of the translated information meaning, precision, or context.

Regardless of the sender or recipient, a common information sharing objective is to communicate high-quality awareness and understanding. In a context as complex as StabOps effective com-

[5] Alberts, David S. 2007. *Agility, Focus, and Convergence: The Future of Command and Control.* Washington: CCRP

munications can be difficult because of the many specialized communities and independent partner organizations that must work together. Information sharing technologies can expose and move information among partners, enabling people to see and interpret (i.e., the power of the web and web pages), but this alone is not sufficient to ensure understanding or achieve process and semantic interoperability. An information/semantic "impedance mismatch" can require manual interpretation (thus precluding automation), reduce the quality of shared information, and reduce the likelihood of shared understanding. Semantic interoperability is important because it enables not only information exchange but also automated processing (e.g., routing, analytics, alerting, and visualization) and process integration.

In Partners We Trust

While trust is an important factor in information sharing, for the purposes of this discussion it will not be addressed. We will assume that each organization has a process and rule set for the release of information and is able to expose to other partners just that which it is willing to share. Similarly, these trust assumptions address information protection considerations, i.e., partner A will not share with partner B information that partner A does not trust partner B to adequately protect (e.g., procedurally and technically) and properly use. Further, we will not address information assurance concerns that arise from both internal and external malicious actions. These factors are all important and must be addressed in any capability development and deployment. Regardless, we will continue here to focus on understanding shared information.[6]

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

Acknowledging Dr. Einstein's advice, what design patterns and standards can help simplify StabOps capability development and improve operational interoperability? Information services are the current architectural paradigm and technology for provisioning information and processing capability to distributed users. When properly designed and implemented, services can be orchestrated to implement business processes enabling people to work together. These executable processes can move beyond information retrieval and manual interpretation and processing. Through well-defined machine-to-machine information exchanges aided, and automated, information sharing and processing become practical.

Web services are a popular style of information service implementation. Like all other types of information systems, web services must address the same familiar fundamental interface and processing design issues. Like all services, there is defined 1) a protocol for interacting and moving bits from "entity" A to B and 2) a specification of what the payload bits mean. Effective robust automated information sharing and processing only occurs when systems are able to reliably move and interpret the bits that have been shared. These "fundamentals" show up in the World

[6] Using well-defined data models as an enabler for policy-based protected sharing capability development is being explored by the Coalition Secure Management and Operations System (COSMOS) Advanced Concept Technology Demonstration (ACTD). This US led multination ACTD (including Australia, Canada, Singapore, Great Britain) is leveraging the formal semantics and structures of the JC3IEDM to robustly define information payloads, operational context, and role-based sharing policies. The policy ontologies define what information is shared with other partners under what contextual conditions (e.g., assigned mission role, location) and are able to reliably filter the information payloads because of shared semantics. The inbound payloads are inspected to ensure they conform to the JC3IEDM schema precluding malicious content. Bilateral VPN links between partners ensure privacy and non-repudiation.

Wide Web Consortium (W3C) definition of a Web Service[7] as shown in Figure 1. Step 1 captures community formation. Step 2 captures the essential specification agreement on protocols and semantics. The semantic specification captures the user domain information exchange requirements. Step 3 represents the development of information service capability based on the agreements developed in step 2. Step 4 shows semantically aligned information systems/services interoperating, and conducting machine-machine information exchanges.

Machine-machine information sharing and understanding shared information is this simple, and not simpler. If the many communities and associated systems and services are engineered to different semantic models then information exchange may be limited and understanding may be compromised. To develop and improve StabOps capability the community must build information systems and services that work together at a level of shared semantic understanding.

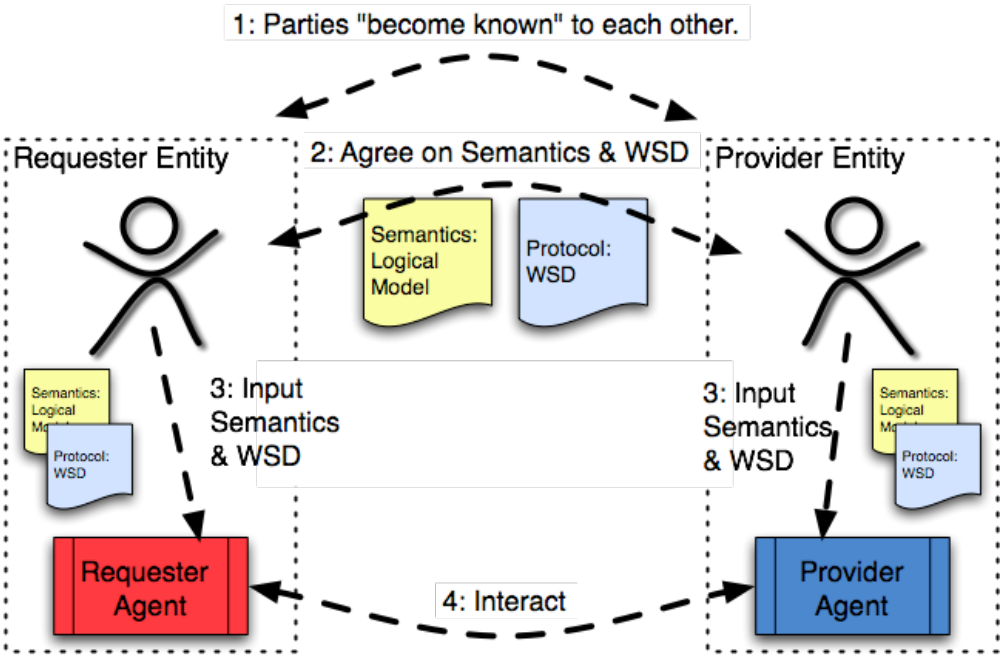


Figure 1. Web Service Operational View

Synchronized Effort

A common organizational and engineering practice is to decompose complex problems. Ensuring that the resulting processes, systems, services and data fit together, operationally and technically, is itself a complex task. It will not happen on its own. Within DoD, the Net-centric Data Strategy (NCDS) has directed the decomposition of DoD information sharing into communities of interest

[7] Web Services Architecture reference document, URL: www.w3.org/TR/wsarch/ "A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Service Description Language - WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."

(COI)[8], each of which is to define business processes, activities, information exchange standards. How each of these community efforts relates to other COIs and how they integrate at the enterprise level is not yet well defined. As a result of legacy acquisition practices and limited guidance, most systems and COIs have developed semantically unique C2 information sharing capabilities. The NCDS initial focus on "discovery" and "access" exposes many of these semantically distinct physical data implementations. Exposing data is a straight forward, useful, initial technical task that decouples data from applications. It is not sufficient to achieve enterprise transformational objectives or joint net-centric capabilities. The DoD Information Sharing Strategy (04 May 2007) notes "numerous independent mission or functional area specific initiatives addressing aspects of information sharing" and goes on to say "**these strategies and efforts must be synchronized in order to achieve unity of effort as well as economic and operational efficiencies**". This insight recognizes, at the enterprise level, the complexity of the problem and the unsatisfactory results of uncoordinated community efforts. It further states the need to focus and converge efforts in order to achieve solutions that provide both operational and economic benefits. Such benefits are most likely to come from harmonization, the resulting simplification, and standardization. What guiding integration patterns should be imposed on decomposition and integration processes in order to ensure that the many functional communities, processes, and tools not only work well in their intended local context, but are able to effectively and efficiently operate and interoperate at an enterprise level? Similarly, what patterns are useful, actually necessary, to work effectively and efficiently with external partners?

An important observation, especially in the StabOps context, is that in isolation no single organization, system or service provides an end-to-end mission capability, rather, each works with many others to achieve effects and objectives. Thus, *integrated capability is the objective capability*. In the net-centric era this implies that the many systems and service components created must interoperate. On the technical side protocols standardize, simplify, and more loosely couple capabilities, e.g., Simple Object Access Protocol (SOAP) and extensible mark-up language (XML) protocols. These technical standards are necessary but are not sufficient because they do not address domain semantic interoperability. Without domain semantic standards the many technical capabilities built may snap together, like so many puzzle pieces, but they will not form a coherent information space, a coherent domain "picture"!

Technical approaches to address domain semantic interoperability gaps are necessary in the short term (to accommodate legacy designs) but are no substitute in the longer term for conceptual and semantic alignment and harmonization among partners. Translation/mapping specifications (e.g., implemented in eXtensible Stylesheet Language Transformation (XSLT) or Web Ontology Language (OWL) Resource Description Framework (RDF) provide mechanisms to deal with syntactic and simple terminology difference. Deeper domain semantic differences can be alluded to but not resolved technically (e.g., A *is similar to* B leaves much unsaid and subsequently unknown when A is translated to B). Ongoing enterprise efforts to develop joint concepts, doctrine and terminology are necessary to get at the root of this problem. Similar operational-level business

[8] "Communities of interest - 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." ref: DOD Net-Centric Data Strategy, DOD Chief Information Officer, 9 May 2003

process analysis efforts with other types of partners are a needed to ensure the understanding of shared information during StabOps.

An Enabling Constraint

Every community spends significant funds to develop systems that enable and support their users. Similarly, each trains personnel in its traditions and specific skills. Each community, including StabOps, has explicit "vocabularies" that are unique. But, in an operational context (e.g., Joint, StabOps) each community must share information with other communities. Thus, as important as community specific languages are, an essential enabling constraint is an enterprise core language - a simplified logical language empowering communities to work together at the joint level. As shown in Figure 2 (each “cloud” conceptually represents a community language) community languages overlap each other. The community overlap concentration can be characterized as a region of joint command, control and coordination concepts and semantics, in short , C2 common core. Each community overlaps this region to a significant degree and extends beyond it. The region represents the information space where these many diverse organizations must be able to share and understand each other.

Figure 3 shows a simplified view of three overlapping communities, one being the Joint C2 community. In the overlaps is where semantic differences create understanding gaps. In the overlap is where harmonization and standardization are essential, but, where too often instead we see duplication and fail to capture operational and economic efficiencies. In the overlaps programmatics and governance issues emerge. Without adequate rationale and criteria to resolve how to organize and reengineer in the overlaps we will not achieve the objective transfomed joint capability. Joint operational requirements set the essential criteria for standardization and integration decisions in the overlap! This rationale creates a clear distinction among communities (i.e., COIs), specifically, joint C2 processes and semantics are the foundation into which other communities must integrate. Figure 3 shows the joint C2 preeminence in shaping information sharing data standards. An essential step is the definition of a shared C2 common core information exchange language. Harmonizing legacy and COI efforts to a C2 common core is an essential enterprise synchronization strategy for achieving semantic interoperability/understanding across national, multinational, and international communities and activities.

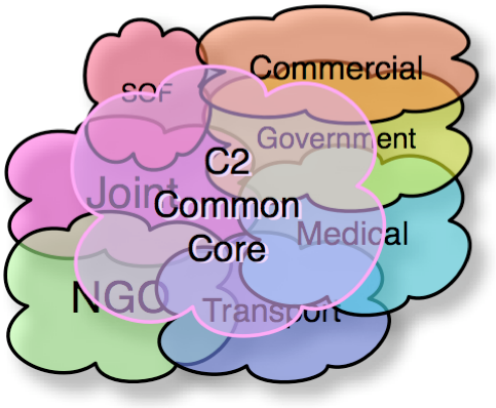


Figure 2. C2 Core and Overlapping Communities

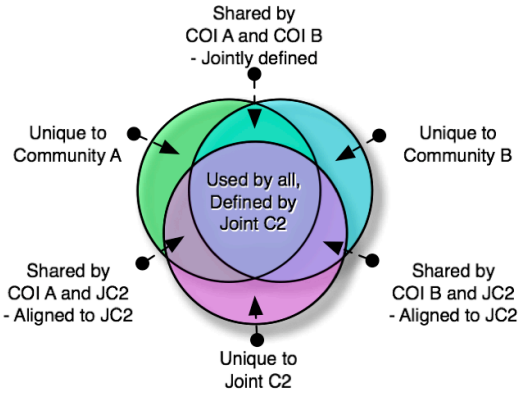


Figure 3. Types of Community Overlaps

A heterogeneous military force can use a shared C2 vocabulary to enable critical information sharing across echelons and communities and to achieve shared awareness and synchronization of effort. During StabOps the scope and type of information that may be exchanged among partners falls largely within the areas familiar to C2 - the C2 core. At a high level, StabOps data semantics include current situation, plans, and status. In the military context, each functional commander/community should be able to share this type of information with other commanders/decision makers as required. Multinational command and control data standards (to be discussed later) effectively cover operational picture data semantics and thus, when leveraged, can greatly benefit the StabOps COI. These same standards can play an essential integrating role, providing semantic interoperability among Service, Joint and multinational commanders. Thus, command and control data standards form the necessary and practical foundation on which to build interoperable and integrated StabOps capability and the supporting net-enabled services.

Many within the joint and multinational C2 community recognize this foundational pattern / requirement and are working to promote it through governance and standard technical solutions. Reusing and extending existing C2 core information standards provides an effective quick start and quick win. Despite this, it will take time and effort to achieve consensus on a predominant C2 core language and to develop community capability that exploits it. In the longer run this approach can promote cost savings, shorten development time and improve delivered capability (truly cheaper, faster, and better). To the contrary, independently defining, implementing and testing of community-specific capabilities will very likely result in service-based stovepipes.

Vision: Integrated Capability

The essential StabOps business process is command, control and coordination. A commander's objectives and guidance must be communicated to subordinates and coordinated with partners. A C2 core language enables community decision makers to share basic operational picture information and to work effectively with subordinates and partners. This minimal, but useful, set of shared C2 concepts and semantics must enable collaborative work with, and among, supporting commanders and other agencies (e.g., planning, coordination, situational awareness, alerting, and status reporting, etc). Operational and tactical C2 information sharing requirements define the core for this shared language for military/StabOps operations.

Figure 4 depicts a generic joint task force and associated C2 information flows. At the top level is an operational commander, supported by (functional area) component commanders conducting planning and coordination and directing mission commanders who are executing specific tasks. This conceptual model is joint, but applies equally well in any functional community. Collaboration processes and techniques enable the planning and execution that must be coordinated horizontally. The vertical and horizontal flow of common C2 type information are essential to enabling effective coordinated operations regardless of community, command and control style, or information sharing technology. Similarly, all efforts are supported by the sharing of situation estimates.

Figure 5 depicts a generic StabOps context and associated information flows. At the top level are executive decision makers, supported by organizational teams that conduct planning, analysis and operations management, and then the actual field teams executing specific tasks. In this conceptual model one stack might represent the multinational JTF (Figure 4), another stack a non-

governmental organization, another stack a governmental agency, etc. It is also appropriate to see each vertical stack as a separate joint component commander and his/her supporting information flows and activities. This model conveys the idea that during StabOps there is a blend of traditional C2 (in the military stacks) and horizontal collaboration (across diverse organizations).

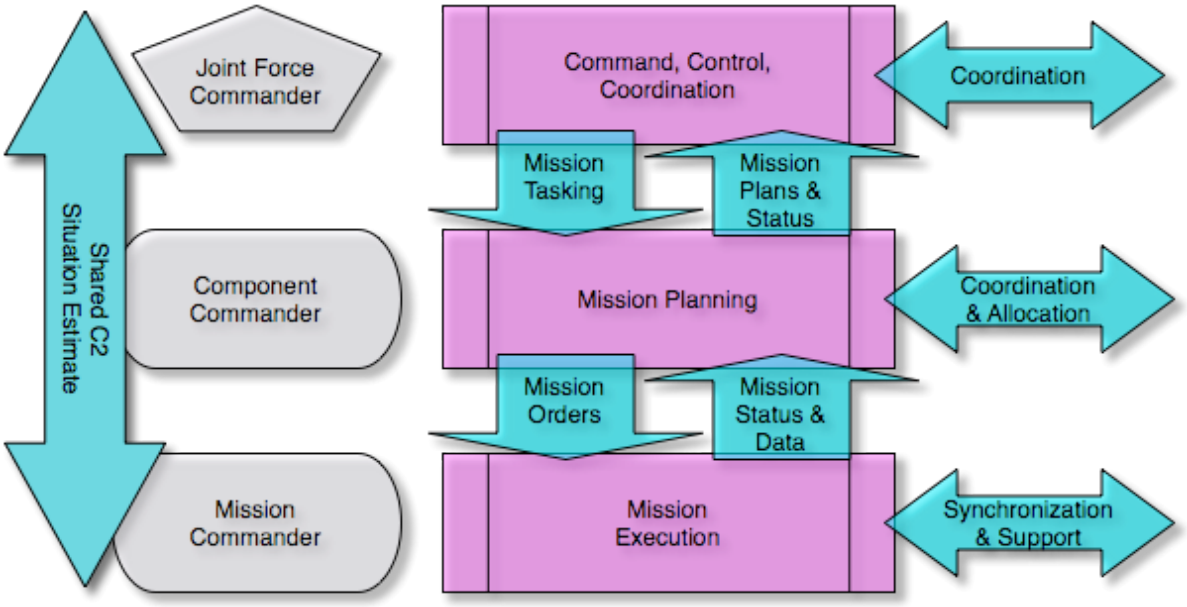


Figure 4: JTF with Command & Control Information Flows

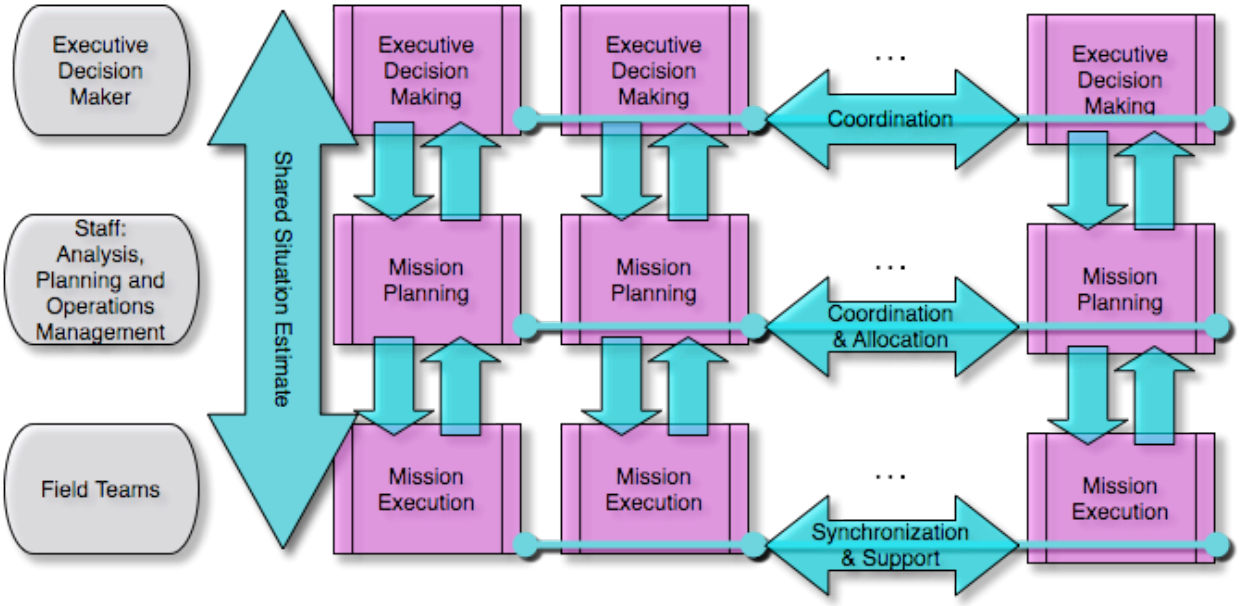


Figure 5: StabOps C2 Information Flows Supporting Coordination and Collaboration

These simplified views are useful in that they help us begin to see common patterns, processes and information sharing needs in the complex business of StabOps. At the top level the shared joint view is essential for basic situation understanding and decision making regarding objectives and coordination. A step lower mission planning, guided by tasking from above, must itself be

coordinated across communities as there is usually a competition for resources. Planning produces detailed community and unit-specific orders for execution at the lowest level. Agility derives from mission command flexibility and confidence in one's understanding of both situation and objectives.

Information technology standardization has made it possible and affordable to link the many organizations and levels shown in Figures 4 and 5. However, many of the activities and much of the information flow shown are today accomplished using manual techniques and unstructured information. Many exchanges require personal liaison techniques that will continue to be essential[9]. Expanding the quality and scope of standard C2 common data can enable and simplify and improved processes and processing where today we have only manual or proprietary solutions.

Under US Joint Forces Command (USJFCOM J87) direction and leadership in March 2008, and in support of the US C2 Capability Portfolio Management Process (C2 CPM), the US started to define a Joint C2 core data model for information exchange. This activity is leveraging an existing, vetted, multinational C2 data standard.

Multinational C2 Data Standardization

The Multinational Interoperability Programme (MIP)[10] is effectively a multinational command and control COI. The MIP membership includes 26 nations, the North Atlantic Treaty Organization (NATO) and Joint Forces Command's Allied Command Transformation (JFCOM ACT). MIP develops and maintains the MIP Common Interface which includes the Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM). In 2007, the US ratified, and NATO adopted the JC3IEDM (STANAG 5525) for C2 information exchange.

Figure 6 gives and overview of the JC3IEDM by showing the independent entities and associations. [11] The generalized / joint content and relationships are evident at this top level. Table 1 shows the independent entity definitions and their role in the model. As may be expected, the JC3IEDM subtype taxonomies and associative relationships (not shown) provide layer upon layer of joint and Service details. The model ensures that these details are semantically derived from the simplified top level view. JC3IEDM is a logical data model that has been driven by operational requirements, abstracted and normalized so as to be neutral with respect to country, Service, system, technology and vendor. In other words, the JC3IEDM is an extensible generalized non-proprietary, open source/standard framework for representing and sharing command and control information. The product of 15+ years of multinational effort it defines and documents the information multinational commanders need to exchange, machine-to-machine, to conduct effective coordinated joint combat and crisis response operations.

[9] Cultural and process norms must be respected. It may never be possible or appropriate to "share tea" over chat instant messaging.

[10] See http://www.mip-site.org

[11] The scope of the JC3IEDM is rich (it contains more than 250 entities, 1000 attributes with more than 12,300 associated defined values). It is more than a lexicon. Important association and sub-typing concepts are represented in an entity-relationship data model. It provides an explicit lexicon, grammar and associated set of domain business rules. It should be noted that JC3IEDM has incorporated STANAG 2014 "Formats for Orders and Designation of Timings, Locations and Boundaries" as the baseline operations orders capability.

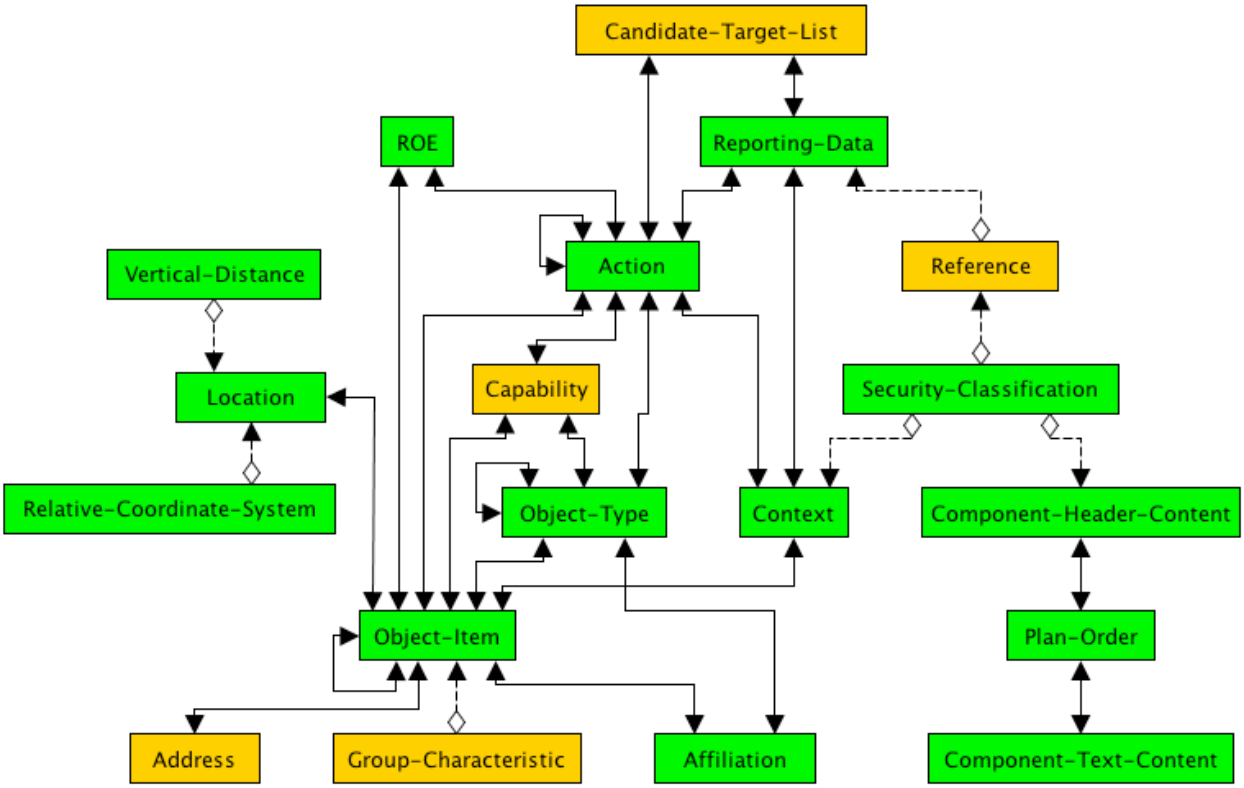


Figure 6. JC3IEDM Independent Entities and Associations

The initial US joint C2 Core efforts have exposed about 1/3 of all of the JC3IEDM elements as a baseline (Figure 6 and Table 1 show in green the exposed JC3IEDM *independent* entities that constitute the initial US C2 Core logical model definition). Continuing efforts will address more C2 requirements and likely adopt more of the JC3IEDM.

Table 1. JC3IEDM Independent Entities and Their Roles[12]

Entity Name	Entity Definition	Role in the Model
ACTION	An activity, or the occurrence of an activity, that may utilize resources and may be focused against an objective. Examples are operation order, operation plan, movement order, movement plan, fire order, fire plan, fire mission, close air support mission, logistics request, event (e.g., incoming unknown aircraft), or incident (e.g., enemy attack).	Dynamics (How, what, when something is to be done, is being done, or has been done.)
ADDRESS	Precise information on the basis of which a physical or electronic destination may be accessed.	Provides means to record postal and electronic addresses.
AFFILIATION	A specification of a country, nationality, ethnic group, functional group, exercise group, or religion to which membership or allegiance may be ascribed.	Provides means to assign affiliations to type or item objects.
CANDIDATE-TARGET-LIST	A list of selected battlespace objects or types that have potential value for destruction or exploitation, nominated by competent authority for consideration in planning battlespace activities.	Information to support ACTION.

[12] The convention is to annotate the names of entities in capital letters and separate words by hyphens. If the name of an entity is used in plural, then a lower-case "s" is appended to the name without changing the name (e.g., the plural of CAPABILITY is written CAPABILITYs).

Entity Name	Entity Definition	Role in the Model
CAPABILITY	The potential ability to do work, perform a function or mission, achieve an objective, or provide a service.	Indication of expected capability for types and actual capability for items
COMPONENT-HEADER-CONTENT	Introductory subject matter intended to identify an element of a plan or order.	Used in conjunction with plan and order specifications.
COMPONENT-TEXT-CONTENT	A textual statement of substantive subject matter.	Used in conjunction with plan and order specifications.
CONTEXT	A collection of information that provides in its entirety the circumstances, conditions, environment, or perspective for a situation.	Multiple roles including grouping of information.
RELATIVE-COORDINATE-SYSTEM	A rectangular frame of reference defined by an origin, x and y axes in the horizontal plane, and a z-axis. The vertical z-axis is normal to the xy-plane with positive direction determined from the right-hand rule when the x-axis is rotated toward the y-axis.	Support to LOCATION for specifying relative geometry.
GROUP-CHARACTERISTIC	A reference to a set of characteristics that may be used for identifying a distinct collection of objects. Examples of characteristics include age group, malady, gender, language, and triage classification.	Supports the counting of types of persons according to selected characteristics.
LOCATION	A specification of position and geometry with respect to a specified horizontal frame of reference and a vertical distance measured from a specified datum. Examples are point, sequence of points, polygonal line, circle, rectangle, ellipse, fan area, polygonal area, sphere, block of space, and cone. LOCATION specifies both location and dimensionality.	Geopositioning of objects and creation of shapes (Where)
OBJECT-ITEM	An individually identified object that has military or civilian significance. Examples are a specific person, a specific item of materiel, a specific geographic feature, a specific coordination measure, or a specific unit.	Identifying individual things. (Who and What)
OBJECT-TYPE	An individually identified class of objects that has military or civilian significance. Examples are a type of person (e.g., by rank), a type of materiel (e.g., self-propelled howitzer), a type of facility (e.g., airfield), a type of feature (e.g., restricted fire area), or a type of organization (e.g., armored division).	Identifying classes of things. (Who and What)
PLAN-ORDER	A planned or ordered scheme worked out beforehand for the accomplishment of an operational objective.	The top-level entity for identification of a plan or order.
REFERENCE	A description of the source from which information, that may have military or civilian significance, is coming.	Pointing to external information in support of REPORTING-DATA.
REPORTING-DATA	The specification of source, quality and timing that applies to reported data.	Support for the reporting function.
RULE-OF-ENGAGEMENT	A specification of mandatory guidance for the way a given activity is to be executed.	Support to ACTION.
SECURITY-CLASSIFICATION	The security classification applicable to an information resource within the domain of classified security information.	Support to CONTEXT, PLAN-ORDER, NETWORK-SERVICE and REFERENCE
VERTICAL-DISTANCE	A specification of the altitude or height of a point or a level as measured with respect to a specified reference datum in the direction normal to the plane that is tangent to the WGS84 ellipsoid of revolution.	Support to LOCATION in specifying elevation or height.

The JC3IEDM (and its predecessor C2IEDM) is officially endorsed by the U.S. Army as the foundation for Battle Command information exchange. JC3IEDM has been adopted as part of the core of the Marine Corps' common information model (CIM) and the foundation on which the Marine Corps Net-Centric Data Strategy is based (excluding business areas). A number of important functional COIs are building on the generic JC3IEDM C2 vocabulary concepts and

elements for their specialized operational needs. These include the DoD Enterprise Global Force Management services, "Chemical, Biological, Radiological, Nuclear, Explosive" (CBRNE) community, and the modeling and simulation (M&S) community which is pressing for increased operation use of M&S through improved interoperability with C2.[13]

When each functional community defines its information sharing capability by building on a C2 common core we establish, in the design phase, the essential foundation for both operational and semantic interoperability. By ensuring that each functional community reuses and extends from core C2 information concepts and semantics we enable horizontal collaboration among decision makers and guidance to flow down and details to flow up without translation. This approach can significantly reduce the number of unique enterprise system, services, and data standards. Some have expressed concern that this approach leads to one large unmanageable model - not true. It leads to many right sized functional COI models that are interoperate (horizontally and vertically) by virtue of a shared understanding of common C2 information.

Enhanced Collaboration

Albert asserts that traditional command and control concepts and terminology must evolve to support the complex coalition StabOps environment and to exploit network enabled information sharing and decision processes.[14] He recommends that *focus* and *convergence* become the new high abstract concepts. "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"[15]. Collaboration is a process in which understanding shared information is essential for establishing common focus and achieving convergence. In turn, it can empower the decision makers to operate in a more agile, timely, and synchronized manner. Collaboration emphasizes information sharing and teamwork, concepts well suited to the heterogeneous StabOps environment. Anybody can be a collaboration partner. In other words, collaboration can occur within and across organizational boundaries, among peers and up and down an organization hierarchy. Collaboration can be planned, periodic, or ad hoc, embodying both classic planning and coordination activities as well as self-synchronization.

The military has recognized the operational value of collaborative information environments (CIE). "CIE: A virtual aggregation of individuals, organizations, systems, infrastructure, and processes to create and share the data, information, and knowledge needed to plan, execute, and assess joint force operations and to enable a commander to make decisions better and faster than the adversary."[16] Today CIE, are typically composed of a collection of applications including; email, chat, instant messaging, common operational picture presentation, shared directories, shared files, voice-over-IP, video teleconferencing, teleconferencing, shared desktops, web por-

[13] See Coalition Battle Management Language (CBML) standardization efforts within the Simulation Interoperability Organization (SISO) and NATO Research Technology Organization, MSG-48.

[14] Alberts, David S. 2007. *Agility, Focus, and Convergence: The Future of Command and Control.* Washington: CCRP

[15] Alberts, Garska, Stein 1999

[16] Operational Implications of the Collaborative Information Environment (CIE), JWFC, Joint Doctrine Series, Pamphlet 5, 1 June 2004

tals/pages, RSS feeds, shared video, whiteboard, and shared calendars.[17] These capabilities are useful but rely mostly on unstructured information limiting the type and degree of automation that can be applied to assist the decision maker (e.g., PowerPoint can not represent a plan in a manner that can be understood by a planning system).

Collaborative work environments (CWE) provide distributed groups of decision makers the ability to cooperate in the performance of common command and control activities. A CWE enables assessments and judgments to be shared with others. A CWE can enhance warfighting capability by facilitating dynamic planning, coordination, allocation, deconfliction, monitoring, alerting, fusion, group assessment, synchronization and reporting. Further, a CWE should support execution across community, echelon, and security boundaries. These types of capabilities are also a key requirement in StabOps operations that inevitably involve diverse DoD, non-DoD agencies, non-governmental agencies and coalition partners.

The US Navy and Marine Corps FORCEnet future capabilities see a need for CWE to exchange and process structured C2 core data:[18]

- "Provide the means collaboratively, and in a timely manner, to create commonly-alterable work products or information objects—such as plans, orders, graphics, analyses, estimates
- Provide the means for decision makers to interact in the comparison and assessment of shared plans, visualizations, work products or other information objects in order to reach mutual understanding."

The Navy and Marine Corp go on to express the additional requirement for C2 systems of very different type and level of sophistication to interoperate with each other and with CIE/CWEs. A CWE, based on a C2 common core data standard would enable better joint and service C2 and StabOps collaborative process by bringing together information from many communities in a common representation. This facilitates improve presentation, analysis and processing.

During a recent US Navy experiment (Trident Warrior 06) the power of a joint C2 common core enhanced CWE was successfully demonstrated. The generic, rich semantic constructs of the JC3IEDM enabled a wide variety of planning activities. Figure 7 shows the simple JC3IEDM-enabled Tactical Collaboration (JTC) application interface that provides this capability. Using the same basic operational planning form a variety of maritime warfare actions were planned, coordinated and shared. JTC enables the real-time synchronous collaboration among many participants who can work together to define, modify, coordinate, consult, deconflict and approve simple standards-based operational tasking documents. The experiment results demonstrated that structured data sharing enhances CWEs in multiple ways. Specifically, the end-to-end plan creation process was much faster, the products were more precise and uniform, and far less bandwidth was required. Additionally, it was demonstrated that JC3IEDM provided a rich standard model for maritime and joint planning and collaboration. Maritime scenarios examined included

[17] Chat is an interesting example of a simple collaboration capability that has found wide acceptance in the public, private and military communities. Despite its limitations, and because of the flexibility of natural language, it has become a standard service on military networks used by many warfare processes.

[18] U.S. Navy and U.S. Marine Corps. *FORCEnet: A Functional Concept for the 21st Century.* Naval Network Warfare Command. Norfolk, VA, 2005.

anti-submarine warfare (ASW), maritime interdiction operations (MIO), land attack (Strike), mine and inshore / amphibious operations (MIW). JTC also translated (with some semantic loss) and presented real-time platform (i.e., ship and aircraft) track data from Global Command and Control System-Maritime (GCCS-M).

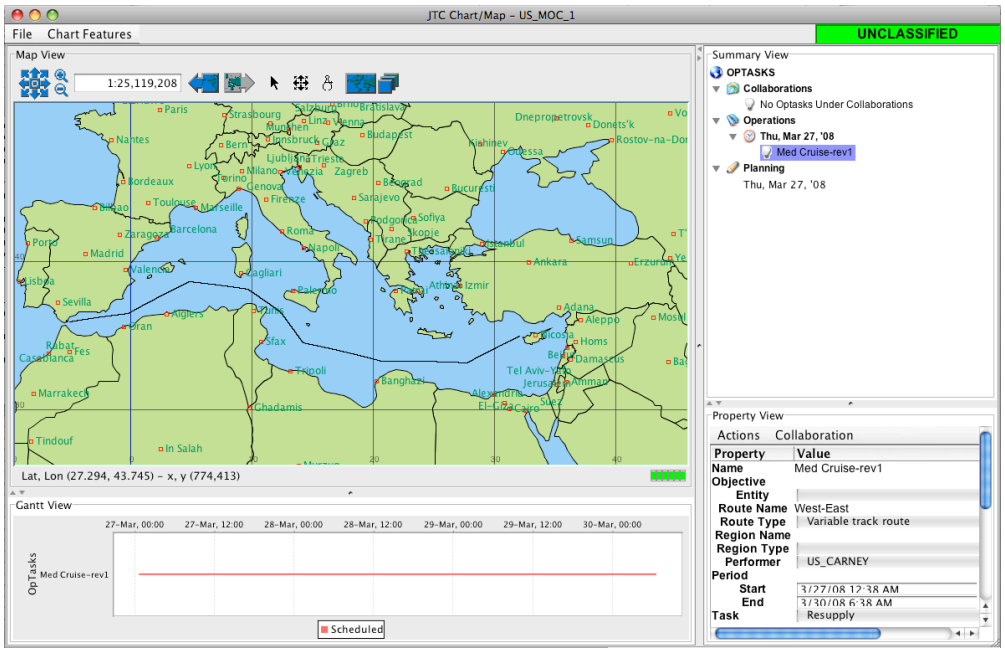


Figure 7. CWE Application: JC3IEDM-enabled Tactical Collaboration (JTC)

Industry Efforts to Enable StabOps Information Sharing

Object Management Group (OMG™) is an international, open membership, not-for-profit computer industry consortium.[19] OMG Task Forces develop enterprise integration standards for a wide range of technologies, and an even wider range of industries. OMG's modeling standards enable powerful visual design, execution and maintenance of software and other processes.

OMGs Consultation, Command, Control, Communications & Intelligence (C4I) Domain Task Force has established an initiative to enhance the ability of first responders, government, military and civilian organizations to develop and sustain a complete, timely and accurate awareness of the operational situation (Common Operational Picture). Referred to as the Shared Operational Picture Exchange Services (SOPES), SOPES will enable users to selectively share information across and between participating organizations; providing an improved visibility of the operational environment affecting decisions and resource commitments. SOPES will enable all participants within a coalition to have the same understanding of the operational scenario and environment within their area of interest. The intent is to provide decision makers with relevant information in near real time while supporting the challenge of tactical communication links. SOPES, in combination with other OMG initiatives, will create a capability that protects sensitive, private, confidential or legally significant information from general dissemination.

[19] http://www.omg.org. Elements of this section are paraphrased from the OMG SOPES request for proposal (RFP).

The shared information environment envisioned by SOPES is categorized by services and/or capabilities supporting a broad cross-section of organizations, including:

- First Responders (e.g., Police, Fire Department and Emergency Medical Personnel);
- Government Agencies (Federal, Provincial/State and Municipal);
- Non-Government Organizations (NGOs);
- Private Volunteer Organizations (PVOs);
- Para-military and security agencies;
- Military (Land, maritime, air, and space).

SOPES will enable a shared representative common operational picture across organizations, agencies and communities of interest (e.g., situational awareness, resource management, logistics, supply, transportation, finance and decision support). SOPES will support diverse political, diplomatic, social and cultural requirements. SOPES capabilities will be useful in information sharing scenarios that address protection of territory, sovereignty, population, and infrastructure from potential man-made or natural disasters, (e.g., natural disaster, medical crisis, terrorist attacks, military operations). Protection includes the concepts of preparation, detection, prevention, response and recovery.

The authors are working within, and with, OSD NII, DDR&E AS&C, MIP, and the OMG to leverage the JC3IEDM as a baseline for SOPES capability. The SOPES JC3IEDM baseline will be undergo OMG balloting in 2008. In this way, the StabOps community can benefit from SOPES industry standardization and products. In turn, SOPES can benefit from the C2 common core work and the semantic interoperability it brings with military organizations.

The Strategy: Engage the StabOps Community

In January 2008, the Integrated Information and Communications Technology (IICT) directorate of the Office of the Assistant Secretary of Defense for Networks and Information Integration (OSD NII) embarked on a path to engage the StabOps community. The IICT intends to leverage lessons learned from the Indian Ocean Basin Tsunami and Operation Unified Assistance. The engagement will be with successful NGO's, IOs, and other US Government agencies with the objective of better understanding and sharing baseline processes and standards for StabOps information sharing. This will include, as appropriate, sharing over the Internet. It will also review activities required to support Humanitarian Assistance / Disaster Relief Operations.

An initial workshop was held at the George Mason University (GMU) School of Public Policy. Respecting some organizational sensitivities to working with US DoD, GMU was chosen as a neutral location and host. The value proposition put to the participants was that StabOps COI efforts and products would enable them to perform their mission more efficiently, with improved safety, and better situational awareness. Further, more efficient information sharing would improve multi-partner processes and coordination and could lead to shortened stability operations. There was an anticipated level of skepticism from the audience with regard to DoD's moving from an information paradigm of "need to know" to "need to share." Reasons for this skepticism vary but the common thread is that the DoD has denied information in the past that was on the critical path for these organizations to succeed. To be frank, operational information disclosure

rules may in the future preclude the sharing of information that others see as essential. It is also true that DoD has had limited means by which to automatically share StabOps information, and limited capacity to manually processes the requests. StabOps data standards will improve the ability to develop services that can find, filter, and automatically share or process information with partners. This improved ability will enable the new paradigm, operational disclosure restrictions not withstanding.

Many organizations have developed their own information sharing solutions that do not involve the DoD. The value of StabOps information exchange standards, and a high degree of interoperability with the US DoD, must be demonstrated to overcome objections and gain support. Through a continuing dialog and interaction trust and shared objectives must be established in order to build an effective StabOps community, with executable processes, useful services and effective data standards.

From a DoD perspective, integrated C2 and StabOps capability establishes the operational context and technical rationale for StabOps information exchange standards. Establishing a StabOps semantic interoperability baseline is a critical effort that will leverage the JC3IEDM, and thus also, the ongoing US joint C2 Core and SOPES work. Admittedly, translation (to be deprecated in the future) will be required as a stop-gap measure. Spiral harmonization / semantic alignment and simplification efforts will be important efforts for some time. Efforts that focus on defining essential processes and interactions it will be challenged to converge on the simple C2 core. Such efforts will also leverage and harmonize with established COI data standards and enterprise services.

The Methodology: Milestones on the Way Ahead

The Stability Operations, like other communities, will undertake a process that brings together the proper stake holders to develop consensus on requirements and acceptable community solutions. The way ahead includes:

1. Engage the community – IOs, NGOs, PVOs, Federal Agencies and the Department of Defense

2. Address critical consensus areas. Work to form collaborative efforts to establish and document options and consensus. Develop, decompose, and harmonize StabOps process and information models. These models become the specifications for services and data. Register products such that the community can review, comment, and test, and improve. Follow DoD guidance regarding the use of Service Oriented Architecture techniques and technologies.

3. Look for opportunities and partners and pilot, validate and iterate the work through participation in demonstrations and exercises. Develop and publish lessons learned and observation feedback.

4. Critique StabOps policies, techniques, tactics, procedures, doctrine, training, and education. Each partner will have a perspective. Assess piloted standards, products and capabilities. Evolve community policies, guidance, doctrine, systems, services, procedures, training, and education migrate to support StabOps standards and enhanced capabilities.

Conclusions

The authors have established rationale for emphasizing semantic interoperability as an essential foundation for the understanding, and automated processing, of information shared during joint and StabOps operations. C2 core semantics have been highlighted as operationally relevant and foundational to every functional community, including StabOps. The recognition and need for cross-community information sharing, and the preeminence of C2 domain, has been presented. C2 Core data standards provide a needed operationally-driven governance/technical methodology of synchronizing COI products and capabilities. Some of the resulting operational and economic benefits have been described. The reuse of the MIP's JC3IEDM has been strongly recommended as a starting point for the StabOps community not the least of which is because of its use in 1) the new proposed US C2 Core data standard, 2) the US Army and Marine Corp net-centric data strategies, 3) the new NATO C3 data standard, and 4) the ongoing OMG SOPES standardization work.

The authors are supporting IICT StabOps initiatives. A Pilot Program, motivated by the Indian Ocean Basin Tsunami and Operation Unified Assistance use cases, is being formulated to mitigate risk and demonstrate useful community capability.

Through these efforts, a sea change may be created that, in the view of all partners working together during StabOps, lowers operational and technical complexity while improving interoperability and capability.

ROUTING SHEET FOR RELEASE OF UNCLASSIFIED TECHNICAL INFORMATION
NUWCDIVNPT 5216/9 (REV. 9-06)

Applicable Classification Guide(s) (see item 2 below): **5513.1F & 5513.4D**

Title of Proposed Release: Making Stability Operations Less Complex While Improving Interoperability

Dated: 4 April 08

Intended for Publication In/Presentation at: ICCRTS Conference Paper, "C2 for Complex Endeavors" [http://www.dodccrp.org/html4/events_13.html]

Type of Information (Check only one item):

☐ Tech Report (TR)/Tech Document (TD) ☐ Tech Memo (TM) ☐ Refereed Journal Article ☐ Other Type of Article

☒ Conference/Symposium Paper ☐ Patent Application ☒ Abstract ☒ Presentation ☐ Poster ☐ Exhibit or Display

☐ Brochure or Pamphlet ☐ CD or Video (indicate content) _____ ☐ Other (specify) _____

Brief Statement of Purpose of Release:
Invited conference paper, re: how the emerging Stability Operations community of interest can leverage an open standard semantic core for multination command and control information sharing. This approach provides an essential, extensible, foundation for communication among international organizations, non-governmental organizations and the military during stability operations.

1. To the best of your knowledge, is the proposed release:	Originator		Technical Reviewer		Dept. Head		OPSEC		01CTO	
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
a. Technically accurate?	☒	☐	☒	☐	☒	☐				
b. Free of critical technology?	☒	☐	☒	☐	☒	☐	☒	☐	☑	☐
c. Free of information with potential intelligence value?	☒	☐	☒	☐	☒	☐	☒	☐	☑	☐
d. Free of information that would adversely affect the security of the U.S.?	☒	☐	☒	☐	☒	☐	☒	☐	☑	☐
e. Considered borderline from being classified?	☐	☒	☐	☒	☐	☒	☐	☒	☐	☑
f. Classified when associated with a known previous release?	☐	☒	☐	☒	☐	☒	☐	☒	☐	☑
g. Liable to damage the success of operation of a system?	☐	☒	☐	☒	☐	☒				
2. Security classification guides have been consulted to ensure no classified or for-official-use-only information (applicable guide(s) to be noted at top of sheet).	☒	☐	☒	☐	☐	☒	☐	☒		

Routing (Name & Code)	Signature and Date	Remarks
Author / Originator Erik Chaum	4/24/08	Sponsor Approved? (Check one) ☒ Yes ☐ No ☐ NA
Technical Reviewer Tom Conrad	Thomas P. Conrad 4/25/08	
Department Head Ernie Correia	Edward Barry for 4/29/08	
OPSEC Officer Pilling, Neil B., Code 553	5/9/08	
Chief Technology Officer Corriveau, Dr. Pierre J., 01CTO	5/15/08	
Public Affairs Officer Sanders, David, Code 01B	5/15/08 ☑ Approved ☐ Disapproved	Approval Stamp (if applicable) DISTRIBUTION STATEMENT "A" Approved for Public Release; distribution is unlimited

Return this package to (name): Linda Casavant **(Code)** 25s **(Bldg)** 1171/3

Note: Originator must send copy of approved releases to Technical Library; e-mail electronic copy to *#NPRI-54-Library-Admin* or send hard copy to Technical Library, Code 5432, Building 101.

☐ **Originator check here to indicate that copy of release has been sent to Technical Library.**

U. S. Department of Defense

Making Stability Operations Less Complex While Improving Interoperability

13th ICCRTS:
C2 for Complex Endeavors
Paper 168

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

Mr. Gerard Christman
OASD(NII) ICCT
(703) 697-8195
Gerard.Christman.ctr@OSD.mil

CCRP

National Security Strategy

"America is now threatened less by conquering states than we are by failing ones."

- In response to this growing challenge, the Department is improving its own capabilities, guided by DoD Directive 3000.05 Military Support to Security, Stability, Transition and Reconstruction Operations.

Stability Operations

- Stability operations involve a range of activities from responding to natural disasters to repairing critical infrastructure and strengthening indigenous institutions to provide security, essential services, justice and economic opportunity.
- Ideally, civilian-led peacetime efforts to help partners improve security and governance can prevent crises. But when major combat occurs, the U.S. and its partners will often inherit the humanitarian, social, and economic problems of the affected state.

Core Military Capability

- StabOps are a core U.S. military mission that the DoD shall be prepared to conduct and support.
  - They shall be given priority comparable to combat operations and be explicitly addressed and integrated across all DoD activities including doctrine, organizations, training, education, exercises, materiel, leadership, personnel, facilities, and planning.
- Stability operations are conducted to help establish order that advances U.S. interests and values.
  - The immediate goal often is to provide the local populace with security, restore essential services, and meet humanitarian needs.
  - The long-term goal is to help develop indigenous capacity for securing essential services, a viable market economy, rule of law, democratic institutions, and a robust civil society.

Complex Endeavor

- StabOps are inherently complex for many reasons:
  - the scale and scope of operations,
  - the variety and interdependence of objectives,
  - the professional and cultural diversity of participants,
  - the types of organizational relationships among participants,
  - the required levels of trust and associated security concerns,
  - operations tempo and often associated time-critical demands on decision makers.
- Additional complexity arises from:
  - environmental factors (e.g., season, region),
  - the wide range of techniques and technologies for information sharing and doctrinal differences in how we choose to organize, coordinate, and synchronize operations.

Fundamental C2 Changes

- Traditional C2 concepts and terminology require fundamental change to effectively perform in coalition combat and StabOps. [Alberts 2007]
  - not amenable to unity of command or a traditional hierarchy organized around strategic, operational and tactical levels
  - unlikely to possess the unity of purpose and discipline that are assumed to be present in a military organization
- While admittedly more loosely organized and coordinated, there remain certain fundamentals
  - partners need to establish collaboration processes, and
  - **understand information exchanged** and effectively manage it in the pursuit of individual and shared goals

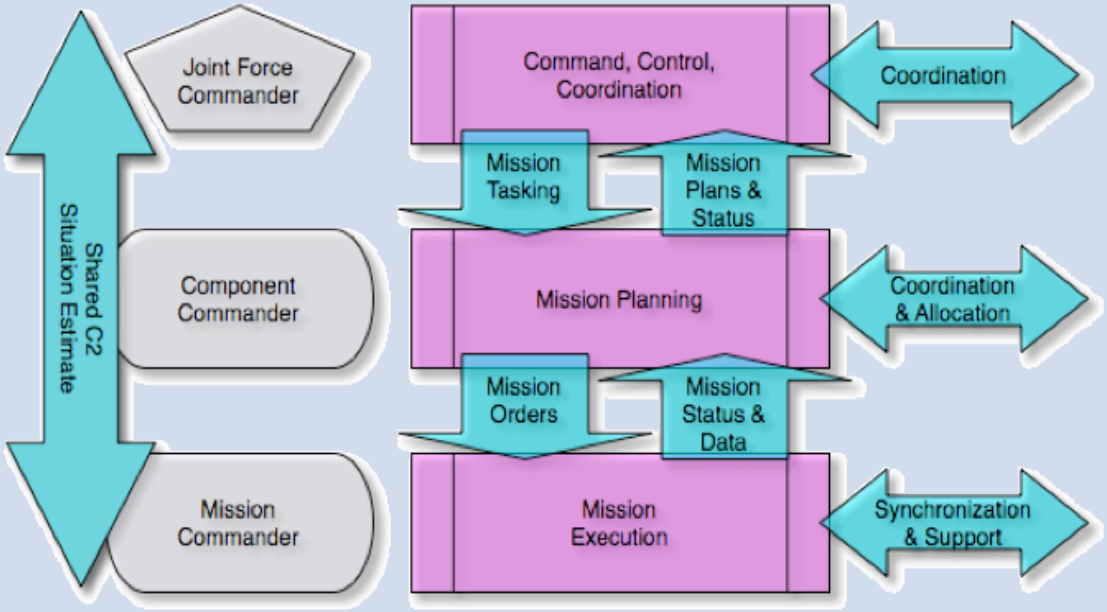
Synchronized Effort

- A common organizational and engineering practice is to decompose complex problems to make them easier to solve.
- This creates the complex problem of ensuring that the resulting processes, systems, services and data fit together, operationally and technically.
- The DoD Information Sharing Strategy† notes:
  - that there have been "numerous independent mission or functional area specific initiatives addressing aspects of information sharing" and goes on to say
  - **"these strategies and efforts must be synchronized in order to achieve unity of effort as well as economic and operational efficiencies"**
- Corollary: No single organization, system or service provides an end-to-end operational mission capability:
  - each works with many others to achieve effects and objectives
  - **integrated capability is the objective capability**

† 04 May 2007

Integrated Capability [1]

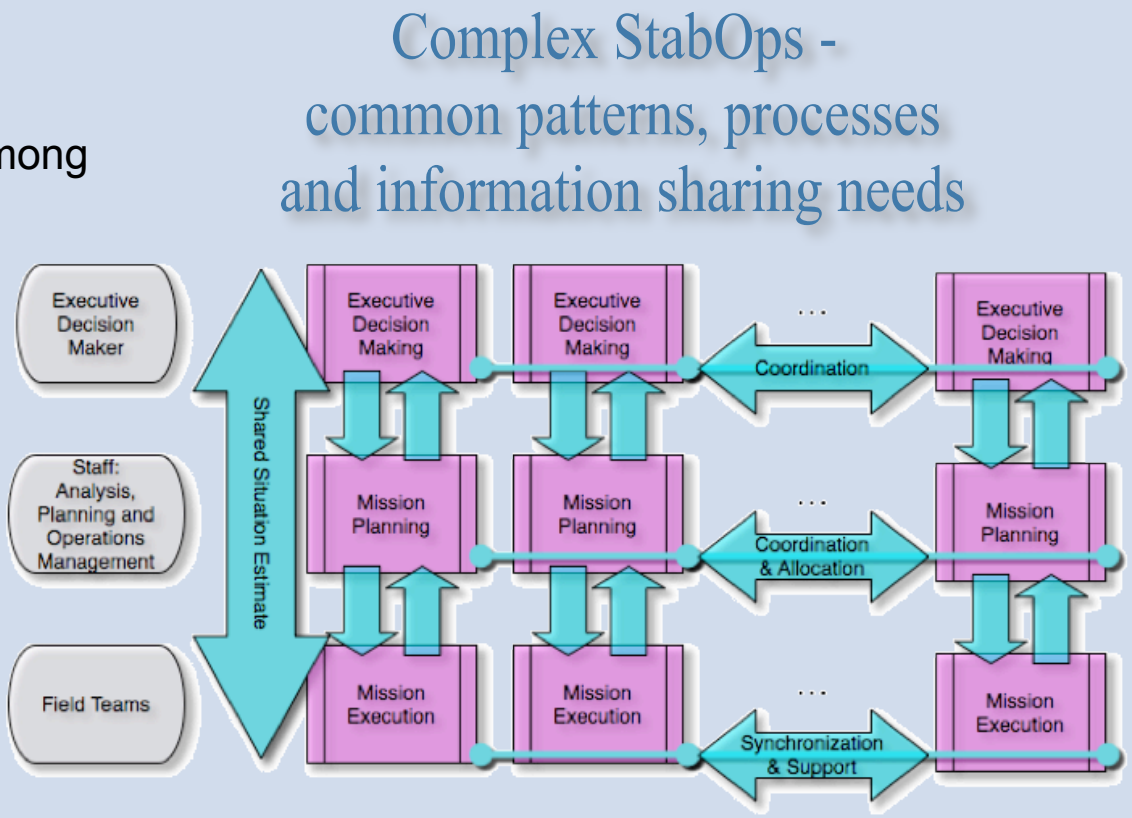
- Generic joint task force and C2 information flows among and between:
  - operational commander,
  - supporting functional area commanders, and
  - mission commanders.
- Information must be understood and flow :
  - Vertically and horizontally
  - SA used at all levels



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

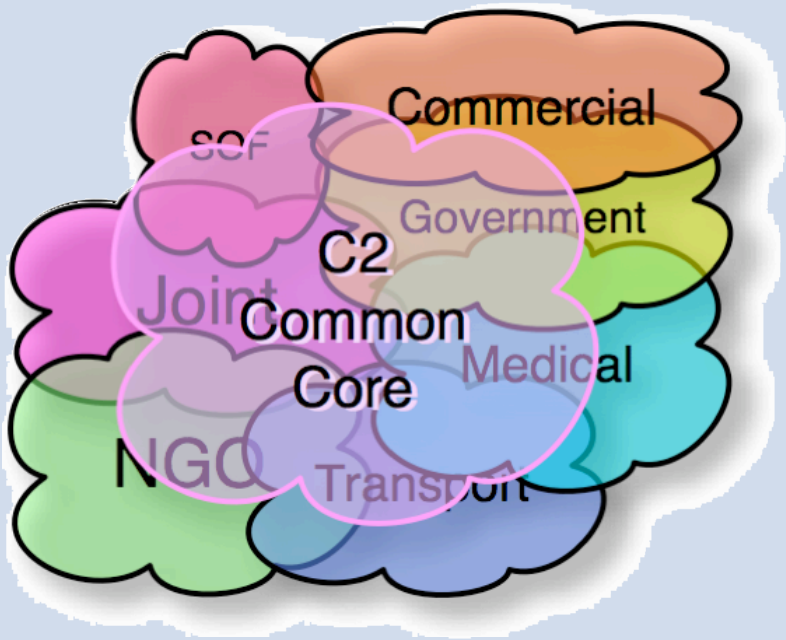
Integrated Capability [2]

- Generic StabOps 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.
- StabOps is 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.



An Enabling Constraint

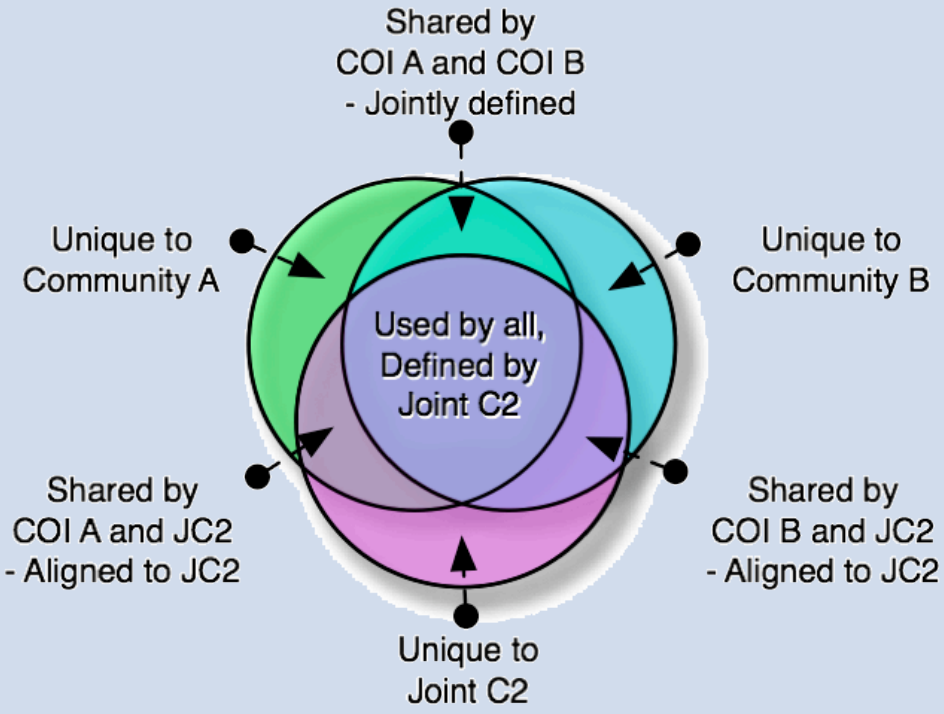
- Community vocabularies are unique, but, overlap!
- In an operational context each community must share information with others.
- All communities use concepts and semantics familiar to C2.
- C2 and collaboration are critical business processes for all.
- An essential **enabling constraint** is a widely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



Each "cloud" conceptually represents a community language.

Cornerstone: Joint C2

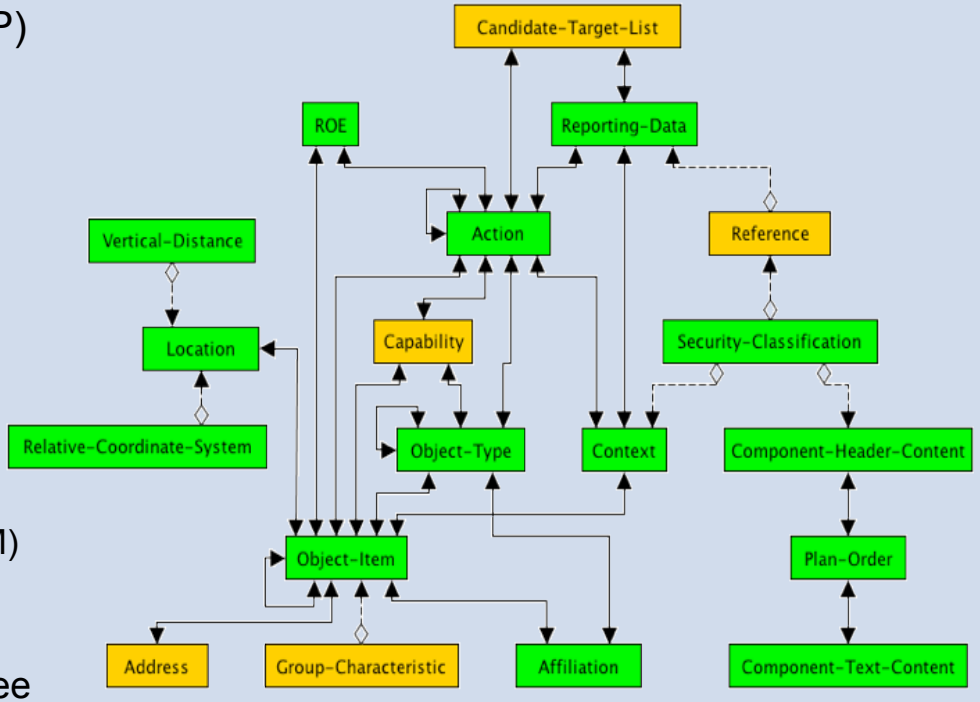
- Overlaps are where:
  - semantic differences create understanding gaps
  - harmonization and standard-ization are essential,
  - too often we see duplication and fail to capture operational and economic efficiencies, and
  - programmatic and governance issues must be addressed.
- We need rationale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



Normalized, Harmonized and Aligned COI Information Sharing

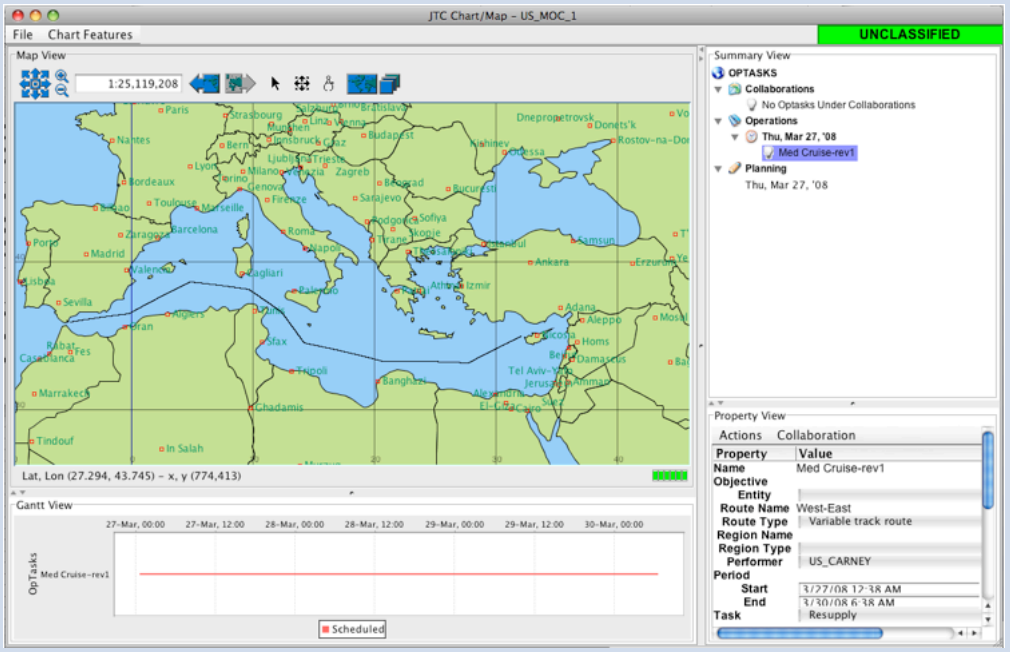
Multinational C2 Core

- Multilateral Interoperability Programme (MIP)
  - 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:
  - Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)
  - Full documentation at: www.MIP-site.org
- USJFCOM (J8) & OASD NII (C2 Policy) oversee the C2 Capability Portfolio Management Process
  - Defining a US Joint C2 core data model for joint, multinational, and StabOps information exchange.
  - Leveraging the JC3IEDM



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-synch- ronization". [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.

Industry: Enabling StabOps

- Object Management Group's (OMG™) Consultation, Command, Control, Communications & Intelligence (C4I) Domain Task Force initiative: Shared Operational Picture Exchange Services (SOPES):
  - enhance the ability of first responders, government, military and civilian organizations to develop and sustain a complete, timely and accurate awareness of the operational situation (Common Operational Picture)
  - enable users to selectively share information across and between participating organizations; providing an improved visibility of the operational environment affecting decisions and resource commitments.
- The shared information services and/or capabilities are intended to support a broad cross-section of organizations, including:
  - First Responders (e.g., Police, Fire Department and Emergency Medical Personnel);
  - Government Agencies (Federal, Provincial/State and Municipal);
  - Non-Government Organizations (NGOs);
  - Private Volunteer Organizations (PVOs);
  - Para-military and security agencies;
  - Military (Land, maritime, air, and space).
- US OASD NII and DDR&E AS&C sponsored preparation of the JC3IEDM submission as a SOPES baseline.
  - OMG and MIP working to build a strategic relationship.
  - Vote expected in Sept 08

OBJECT MANAGEMENT GROUP

MISSION: To produce and maintain computer industry specifications for interoperable that will support a full-lifecycle approach to enterprise integration which maximizes ROI.

Engage the StabOps Community

- Objective: improve DoD support of StabOps
  - Engage successful NGO's, IOs, and other US Government agencies and establish baseline processes and standards for StabOps information sharing
  - Leverage lessons learned from the Indian Ocean Basin Tsunami and Operation Unified Assistance - Humanitarian Assistance / Disaster Relief Operations
  - Proponent - OSD NII, Integrated Information and Communications Technology (IICT)
- Value proposition - COI efforts, information sharing standards, and products will enable the community to:
  - perform missions more efficiently and in a more coordinated manner
  - enhance all partner's situational awareness, operational safety, and security
  - shortened stability operations
- Need to build relationships and trust within the community
  - skepticism - i.e., DoD's move from "need to know" to "need to share."
- StabOps information sharing improvements needed to enable a new paradigm:
  - operational disclosure restrictions, and the continuing need for direct person-person liaison not withstanding, current information sharing methods and processes are too manual, too slow, and too ad hoc
  - Information sharing standards will enable partners to define and field services that can find, filter, and more easily share, or process, information with other partners
  - Leverage MIP JC3IEDM and OMG SOPES

Milestones on the Way Ahead

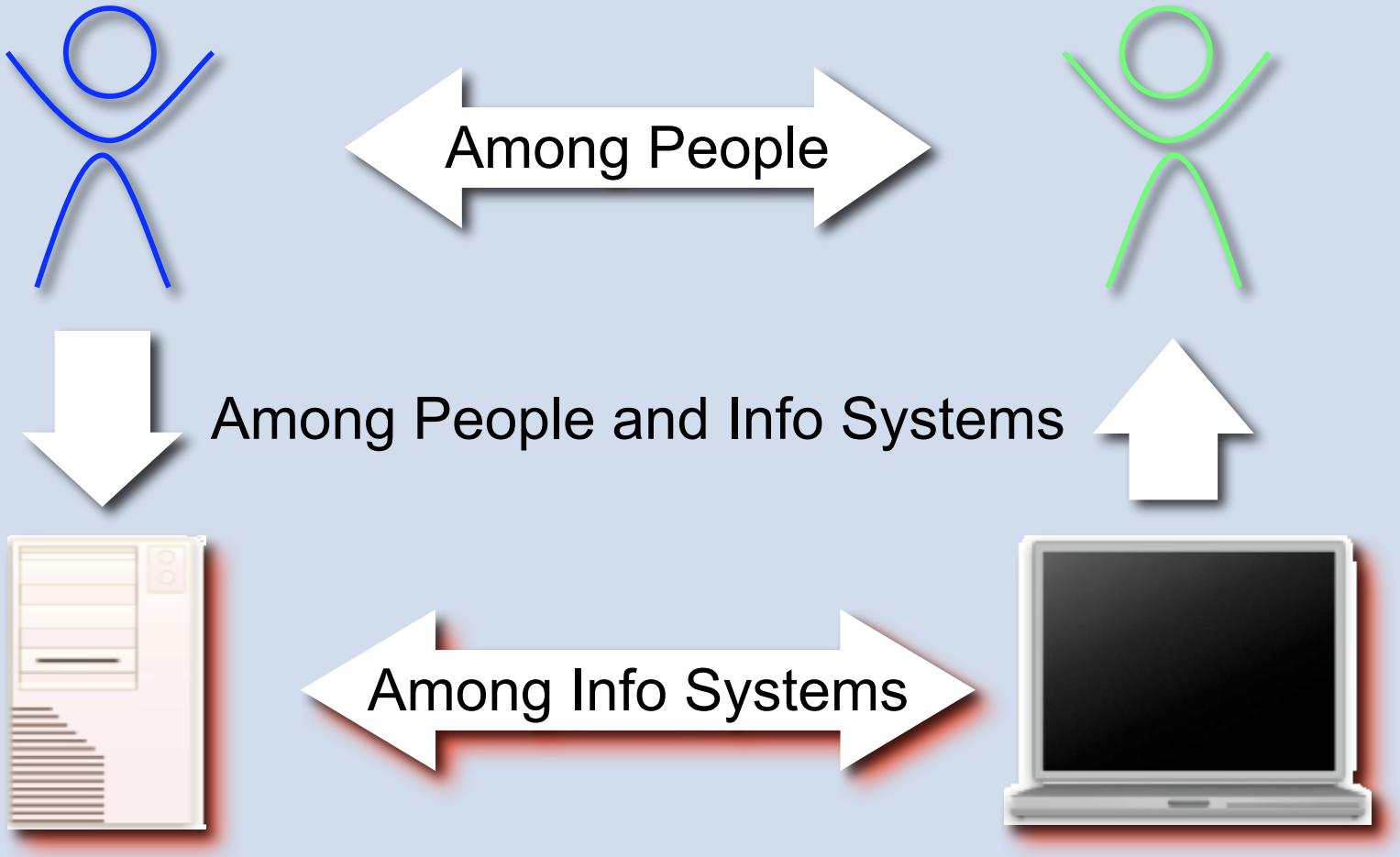
- Begin to bring together diverse stakeholders to develop consensus on requirements and community solutions. The way ahead includes:
  - Form or partner with ongoing community efforts that include
    - IOs, NGOs, PVOs, Federal Agencies
  - Develop, decompose, and harmonize StabOps process
    - Build awareness of partner policies, techniques, procedures, doctrine, training and required capabilities
    - Build consensus on useful shared community products and capabilities
  - Develop, decompose, and harmonize information models.
    - Models enable specification of services.
    - Follow DoD guidance regarding the use of Service Oriented Architecture techniques and technologies. Register products for review, comment, test, and improve.
    - Leverage industry efforts
  - Pilot, validate and iterate the work through participation in demonstrations and exercises

Conclusion

- Stability Operations are complex, but, appropriate information standards will reduce complexity and improve capability.
  - Strive for semantic interoperability, an essential foundation for the understanding, and automated processing, of information shared during joint and StabOps operations.
  - Leverage standard C2 core semantics - operationally relevant and foundational to every functional community, including StabOps
  - Recognize the preeminence and role of a standard C2 core semantics as a foundation for cross-community information sharing
- C2 Core data standards provide a necessary, operationally-driven, governance/technical methodology for synchronizing intra and inter-COI products and capabilities.
  - StabOps must mesh effectively with military operations
  - Leverage JC3IEDM (NATO STANAG 5525 and soon to be offered as OMG's SOPES) as a standard C2 core semantic baseline for StabOps
- Address StabOps community information sharing needs
  - Work to enable StabOps partners to work together more effectively in the field by lowering operational and technical complexity while improving interoperability and capability

Back-up

Types of Information Sharing



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