A Proposal For A Department Of Defense (DoD) Command And Control Strategy

Alfred V. Newman and Ross W. Wheelwright

Introduction

The evolution of C2 functionality to Net-Centric Warfare is well underway. Command and Control (C2) is already being operated as a Net-Centric function today.

We will outline suggested changes to the development approach necessary to build Joint Command and Control (JC2) systems as part of an overall Net-Centric C2 enterprise.

Proposed DoD C2 Strategy – Major Tenants

The proposed DoD C2 strategy has four major tenants:

1) Continuous operational evolution to net-centric warfare,
2) Ubiquitous user connectivity to distributed, authoritative data,
3) Dynamic command and control capability growth, and
4) Incremental change built upon a near term implementation.

To evolve C2, it is necessary that a continuous operational evolution to net-centric warfare take place. We must focus on DoD C2 as the major force multiplier of Net-Centric Warfare. This focus will enable accelerated evolution of DOTMLPF changes across the DoD C2 enterprise. By providing all users, with shared access to C2 information, regardless of COCOM boundaries, will enable new levels of collaboration and sense making which are not possible today. This top to bottom, POTUS to soldier, distributed information environment for C2 decision making is a key enabler of the National Command Capability (NCC) required by Presidential directive.

By providing a robust DoD C2 Services Oriented Architecture (SOA) the Military Departments (MILDEP) will be more capable of developing truly unique C2 needs without duplication and expense of development and sustainment of unique software and hardware.

Ubiquitous user connectivity to distributed, authoritative data will provide to users at all levels across the GIG network secure, robust, assured information flow. Users at all levels from fixed C2 centers and deployed in mobile C2 centers, from POTUS to an individual solder, will have access to the same distributed, authoritative data. To achieve this ubiquitous user connectivity the GIG network must provide full spectrum security that enables aggressive counterintelligence. Providing for the “need to share” as the replacement to “need to know” and stepping up to aggressively attacking the “insider threat” of cleared users requires an overall GIG network with full spectrum security.

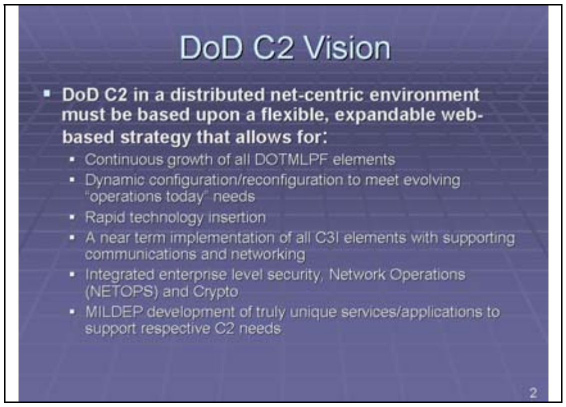
To achieve the desired rapid evolution of C2 to net-centric warfare, a very dynamic command and control capability growth must evolve worldwide. The new JCIDS process, required by Title X law, provides validated requirements. When these requirements are prioritized by the COCOM's in an organized forum based upon current and projected operational needs, C2 will be capable of rapid evolution.

As stated in DPG 2003, but still in process of implementation, the DoD is evolving from systems based development to capabilities based acquisition. When DoD C2 capabilities are built-up based upon a DoD C2 SOA, the C2 capabilities can be acquired and integrated into an overall National Command Capability that is capable of dynamic configuration/reconfiguration of hardware, software and networking/communications. This rapid fielding of C2 capabilities based upon "current operations" prioritization by the COCOM's provides the Net-Centric foundation of the DoD C2 enterprise.

The formal Analysis of Alternatives (AoA) for the JC2 program indicated that, without a fundamental change in the traditional DoD C2 acquisition and fielding, it will be 2020 before JC2 can be fielded. Waiting until 2020 to have a fully operational replacement capability for GCCS is simply not acceptable. Instead, we propose a systems engineering approach for the DoD C2 environment that provides for incremental change built upon a near term implementation. The proposed DoD C2 environment provides for rapid technology and C2 capability insertion into the operational worldwide warfighting system.

DoD Command and Control Strategy – Essential Elements Of Success

Figure 1 lists the essential elements of success for evolving the proposed DoD C2 flexible, expandable, web-based strategy. This list of elements can form the basis for the future evolution of Net-Centric C2 in terms of DoD Directives, Instructions, Training, Tactics, Procedures (TTP).



DoD C2 Vision

- DoD C2 in a distributed net-centric environment must be based upon a flexible, expandable web-based strategy that allows for:
  - Continuous growth of all DOTMLPF elements
  - Dynamic configuration/reconfiguration to meet evolving "operations today" needs
  - Rapid technology insertion
  - A near term implementation of all C3I elements with supporting communications and networking
  - Integrated enterprise level security, Network Operations (NETOPS) and Crypto
  - MILDEP development of truly unique services/applications to support respective C2 needs

2

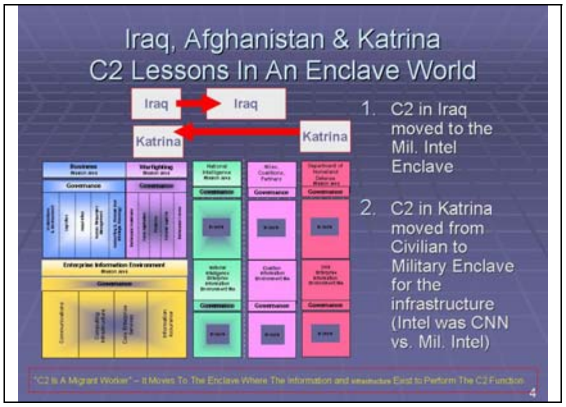
Figure 1

Net-Centricity is a key enabler that allows a C2 capability to operate in the Joint Vision 2020 world of Force Protection and minimally sized forward footprints. Net-Centricity does not eliminate the need for C2, but C2 situational awareness and decision-making are facilitated and enabled by Net-Centricity. The challenge today is to rapidly evolve the TTP necessary to effectively enable C2 capabilities to operate in the world of Net-Centric Operations and Warfare

Katrina lessons learned

C2, as an inherent capability, must interface with many sources of information to develop military courses of action in response to threats on the battlefield. Figure 2 provides the notion that C2 dwells in an enclave world of information domains.

As shown, C2 in IRAQ moved to where the information could be received and transmitted to the Intelligence and secure communications domains. C2 moved out of the Command Center to the Intelligence Center, because that was where the Joint Task Force commander was able to get the integrated information he required to execute his battle plan.


Iraq, Afghanistan & Katrina
C2 Lessons In An Enclave World

1. C2 in Iraq moved to the Mil. Intel Enclave
2. C2 in Katrina moved from Civilian to Military Enclave for the infrastructure (Intel was CNN vs. Mil. Intel)

"C2 Is A Migrant Worker" – It Moves To The Enclave Where The Information and Infrastructure Exist to Perform The C2 Function

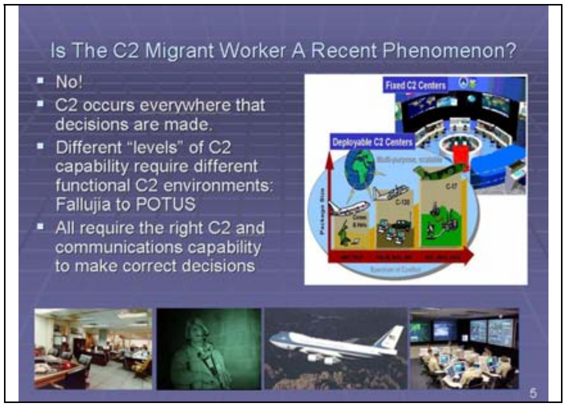
Figure 2

On the other hand, C2 military support to the KATRINA hurricane disaster in New Orleans, Louisiana moved from the Homeland Security domain to the C2 military domain (Figure 2) because the JTF commander had access to all the information he needed, including intelligence information from CNN, and a communications infrastructure that worked.

The civilian capability to perform command and control (fire and police actions) was destroyed and the military were able to respond by deploying a mobile C2 center, the amphibious ship, IWO JIMA.

Command and Control as a Mobile User

C2 exists anywhere that a situationally aware decision is being made or contemplated as seen in Figure 3. A person working at a computer somewhere in the world and a soldier talking on a radio while peering around the corner of a building in Falluja, Iraq, are both examples of C2 functions operating within a distributed environment in which the C2 SOA operates.


Is The C2 Migrant Worker A Recent Phenomenon?

- No!
- C2 occurs everywhere that decisions are made.
- Different "levels" of C2 capability require different functional C2 environments: Fallujia to POTUS
- All require the right C2 and communications capability to make correct decisions

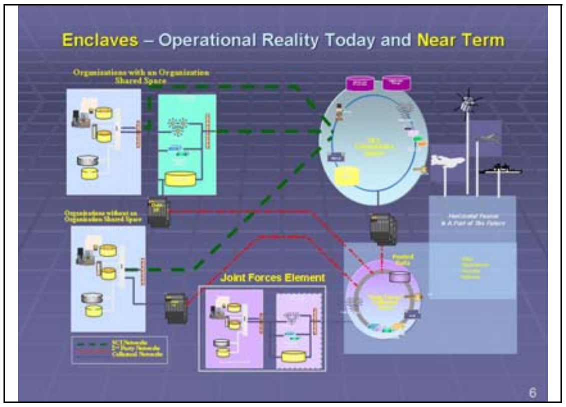
Figure 3

Command and Control is inherently a mobile function that must be performed wherever C2 decisions must be made. Thus, we must recognize that the C2 users and decision makers are inherently mobile and constantly migrating to wherever the C2 decision-making must be performed.

Mobile users from POTUS to a solder in combat cannot be left behind by C2 or Communications infrastructure as they move within either homeland defense or any other part of the Range of Military Operations (ROMO). The conduct of DoD C2 cannot be limited by Line of Sight (LOS) communications, fiber optical cable lay down or any other infrastructure limitations.

DoD C2, as it evolves to Net-Centric Warfare, must become as mobile as is required by its most demanding users, but it must also include a complementary fixed C2 infrastructure to minimize the number of mobile C2 users that must be forward deployed.

The fact that one person has a computer (IT), and the other does not, is not a distinguishing characteristic of C2. Both IT and communications capabilities enable decision makers to accomplish their C2 missions with the best possible situational awareness and knowledge of all relevant factors in their decision.


Enclaves – Operational Reality Today and Near Term

Organizations with an Organization Shared Space
Organizations without an Organization Shared Space
Joint Forces Element
6

Figure 4

C2, inherently, must be capable of interfacing with many sources of information to develop military courses of action in response to threats on the battlefield. Figure 4 provides the notion that C2 dwells in an enclave world of information domains. While work has been done to create an information environment for C2 in a multi-level security environment, that environment is not fielded today or scheduled for fielding.

Thus, our proposed DoD C2 strategy is based upon an acceptance of the current security enclave environment in which Command and Control must currently exist. We must proceed to field C2 capabilities in our existing enclave security environment and allow for information flow to decision makers.

This does not mean that a "sneaker-net"[1] should be tolerated or required in a net-centric C2 environment of the future. Enclaves are, however, the common accredited security environment in which C2 must exist today. In order to move to more rapid fielding of C2 capability it is necessary to accept, and even embrace the existing enclave nature of DoD networks in order to move forward rapidly to a implementation of JC2 worldwide in the near term.

When multi-level computing and networks are available, they should be fielded as capability improvements in infrastructure to the mobile C2 users. Not having to provision, transport, maintain and use multiple computers for C2 on separate networks would benefit the mobile C2 and combat users. Until "MLS security" exists in fieldable form, we must provide to all C2 decision makers and the forces they command the situational awareness capability required.

What does C2 look like in a Net-Centric Environment?

In recent years there has been much debate about what C2 in a net-centric environment looks like and includes. In the domains of C2 and Intelligence, one normally finds that the command nodes consist of fixed or mobile nodes. Some of these nodes are familiar such as, AWACS, the White House, Air Force 1 and CENTCOM Headquarters, as shown in Figure 5.

Moving toward Net-Centric Warfare does not eliminate the need for either fixed or mobile C2 centers. Both have a part in the Net-Centric future. Force protection principles now in place for over 10 years state that the mobile forward deployed force should be as minimally sized as possible. This means that small very mobile command posts, larger JTF mobile command posts and fixed command posts at COCOM locations are all necessary to enable distributed C2 across the Net-Centric enabled battlefield.

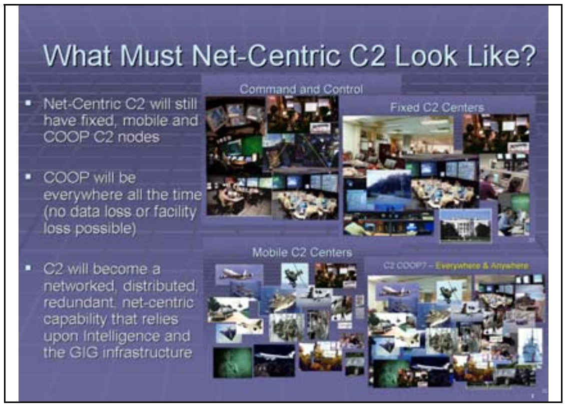
Some have tried to curtail the upgrade of fixed C2 centers worldwide. The rationale used was that fixed C2 centers are merely targets and worse, examples of the lack of implementation of Net-Centric operations principles. However, even when an individual sitting at a computer somewhere in the world, attached to the GIG, provides essential functions in support of Net-Centric warfare, the need for some fixed C2 centers is not eliminated.

Recent USJFCOM decomposition of the Joint Task Force HQ (JTF-HQ) Joint Mission Thread (JMT) has resulted in some 1600 tasks being identified. Coordinating and executing this number of tasks requires some level of organization, command, and control, even in Net-Centric Warfare.

Thus, the future of C2 in Net-Centric Operations will continue to have fixed and mobile sites. A C2 fixed or mobile site can be as small as a single person or team performing a required function, as long as that function is coordinated, and integrated into the overall Net-Centric mission being performed.

Having Continuity of Operations (COOP) as a built-in capability of the future DoD C2 enterprise minimizes, as far as possible, the size, complexity and targeting value of fixed C2 infrastructure. In a Net-Centric future, C2 for Continuity Of Operations (COOP) exists anywhere, distributed across the world.

Losing any physical facility, fixed or mobile, must result in the loss of zero information and capability to the overall DoD C2 enterprise. The commercial marketplace has already evolved into this type of truly distributed operations environment. Achieving COOP by backup of selected data elements is a rudimentary, but insufficient version of COOP.



What Must Net-Centric C2 Look Like?

- Net-Centric C2 will still have fixed, mobile and COOP C2 nodes
- COOP will be everywhere all the time (no data loss or facility loss possible)
- C2 will become a networked, distributed, redundant, net-centric capability that relies upon Intelligence and the GIG infrastructure

Figure 5

Where does the C2 domain belong?

Operationally, Command and Control has military and even civilian components depending upon the Range Of Military Operations (ROMO). Simply drawing a chart and putting "Command and Control somewhere" is not a trivial task. Katrina and Operation Iraqi Freedom (OIF) lessons learned indicate that both C2 and Intelligence are enterprise-wide entities that exist as functional capabilities above the Domain and Enterprise Services levels of the Domain model. Since C2 moves, it in fact exists across the enterprise, as shown in Figure 6. Multi-national operations, disaster relief, conventional and unconventional warfare all require that C2 remain mobile, agile and operational regardless of the physical and logistical constrains imposed by a given operational condition.

C2 is not simply in the military domain, but exists as well in the complex Posse Comitatus Act of 1878 environment in which DHS found itself after Hurricane Katrina and Rita. The DoD military cannot simply run operations and "command" civilians without a request from local and state officials. While most police, fire and first-responders understand, implicitly, the function and need for effective C2, the implications of the term "command" in a mixed military and civilian environment are non-trivial.

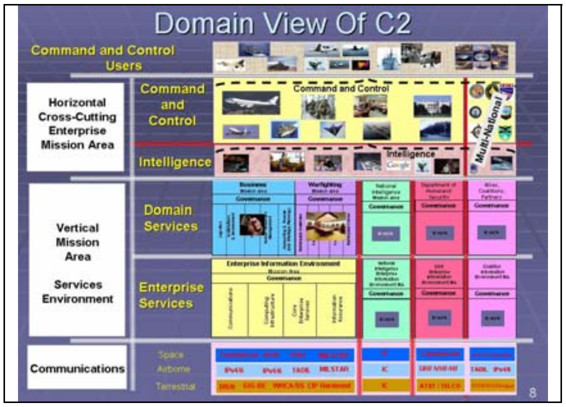


Figure 6

Command and Control Strategy Concepts and Roadmaps

In recent years, a number of essential efforts have been underway in the DoD to roadmap and bring structure to Command and Control in the DoD. This acknowledgement of the need for evolving C2 concepts and expressing those changes into rational roadmaps has led to a number of efforts, as shown in Figure 7. As the various concepts and roadmaps have evolved, a degree of overlap and conflict in scoping and executing these concepts as execution roadmaps has surfaced.

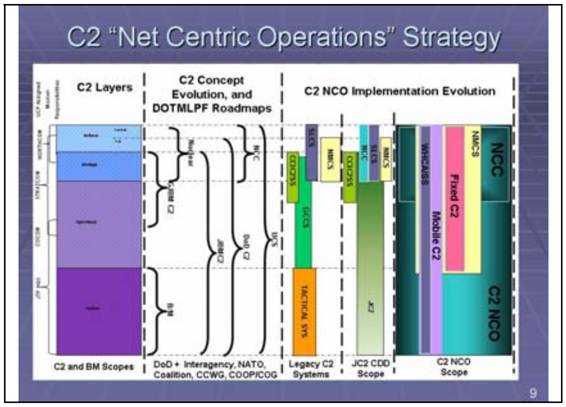


Figure 7

In order to integrate these concepts and enable the evolution towards net centric operations, it is necessary to provide a functional framework in which C2 evolves. We propose the use of a Services Oriented Architecture (SOA) as the framework for integrating C2 in its evolution to the Net-Centric future.

C2 Service Oriented Architecture (SOA)

Service-oriented architectures are not a new concept. We suggest in this paper that C2 functionality in the Net-Centric environment may be best described in terms of a Services Oriented Architecture (SOA) that supports C2 services and applications much like a computer operating system supports various software applications.

A C2 SOA allows C2 functionality in the form of services and applications to be available within this Net-Centric environment. The execution of C2 is inextricably connected with intelligence (also identified as information source in the IT world). This information exchange is known as the OPS-INTEL interface and has, historically, been of one of the most difficult for C2 to exploit.

Because a C2 SOA is based upon loosely coupled services rather than tightly coupled integrations, service oriented infrastructures and applications can change as quickly as C2 needs change. Services can be constructed, deployed, and reused virtually on demand, and easily integrated enterprise-wide, across heterogeneous platforms.

Accordingly, a C2 SOA, as shown in Figure 8, is essentially a collection of C2 services (C2 Missions and Tasks). These services (tasks) communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed.

The implementation of the C2 SOA can yield a cost-effective, efficient integration of systems and processes, because it lets organizations rationalize and reuse services and easily automate processes based upon those services. A C2 SOA directly addresses two key burdens of existing C2 IT environments – lack of leverage across existing systems and high maintenance costs.

In a C2 SOA environment, nodes on a network make resources available to other participants in the network as independent services that the participants access in a standardized way. Most definitions of SOA identify the use of Web services in its implementation. However, one can implement a SOA using any service-based technology.

The software components become very reusable because the interface is defined in a standards-compliant manner. The C2 SOA can provide a methodology and framework for documenting enterprise capabilities and can support integration and consolidation activities.

A C2 service is a self-contained, stateless computer function that accepts one or more requests and returns one or more responses through a well-defined, standard interface. Services should not depend on the state of other functions or processes. The technology used to provide the service, such as a programming language, does not form part of this definition.

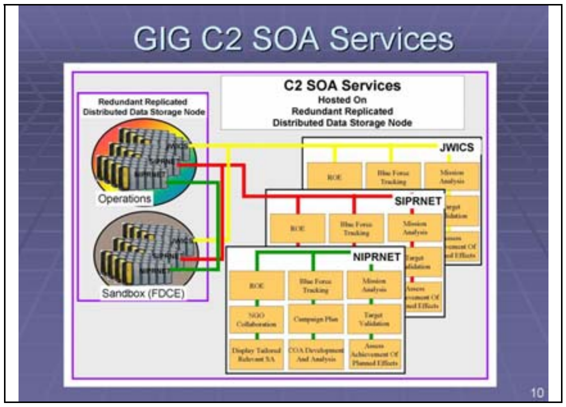


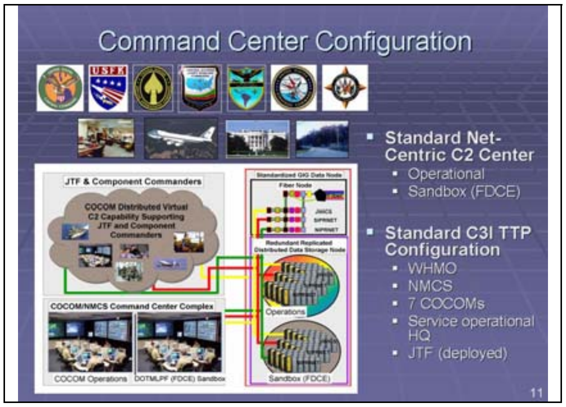
Figure 8

A DoD C2 service exists on a DoD network. In fact, it should exist on each of the DoD networks, as shown in Figure 8, in order to provide commonality in capability, training and execution. As shown in Iraq and Katrina the mobile nature of C2 necessitates having fully functional C2 capabilities on each of DoD's networks.

A C2 service oriented architecture relies on the ability to identify services and their capabilities. Therefore, a C2 SOA depends on a discovery service that describes the other services available in this domain. When most people speak of a SOA, they speak of a set of services residing on the Internet or an intranet using "Web services." Everyone knows roughly what a "web service" is, but there is no universally accepted definition. Despite the difficulty of defining web services, it is generally accepted that a web service is a SOA.[2]

C2 Integrating Concept

In Figure 9 a C2 COCOM command center complex is shown for discussion purposes as having two components, the operational command center and the development and test center (Sandbox). Both the command center and the development and test center are supported by common communications and data infrastructure.



Command Center Configuration

- Standard Net-Centric C2 Center
  - Operational
  - Sandbox (FDCE)
- Standard C3I TTP Configuration
  - WHMO
  - NMCS
  - 7 COCOMs
  - Service operational HQ
  - JTF (deployed)

USFK
JTF & Component Commanders
COCOM Distributed Virtual C2 Capability Supporting JTF and Component Commanders
COCOM/NMCS Command Center Complex
COCOM Operations
DOTMLPF (FDCE) Sandbox
Standardized GIG Data Node
Fiber Node
JWICS
SIPRNET
NIPRNET
Redundant Replicated Distributed Data Storage Node
Operations
Sandbox (FDCE)
11

Figure 9

In order to ensure that future TTPs development does not degrade into "reach-forward" from "reach-back," the "Sandboxes" will only exchange information with other "Sandboxes" at other sites. This TTP "Sandbox" evolution is required to transition C2 into the world of Net-Centric Warfare.

The real military doctrine fear of returning to centralized C2 has previously driven operational concepts and capabilities into an environment in which the National Military Command System (NMCS) has limited visibility and intentionally limited control over operations within a given COCOM/JTF operation.

The current Combatant Commands (COCOM's) were once operated by Commander In Chief's (CINC's) and had specified statutory authorities. Under the current Unified Command Plan (UCP) there is only one Commander in Chief and that is POTUS, the President of the United States.[3]

As part of the recent C2 evolution the term "National Command Authority" has been ordered discontinued[4]. The term originates in the Unified Command Plan as is defined as "the President and the Secretary of Defense, or their duly deputized alternates and successors" and has been replaced with "the President" or the "Secretary of Defense" or both, as appropriate.

Evolution Of Net Centric C2

Operation Enduring Freedom (OEF) in Afghanistan taught brought out important leadership obligations that come as part of Net-Centric C2. Unprecedented close connectivity, as exists in a Net-Centric world, however, can cut both ways. Although Global connectivity was helpful--and even essential--up to a point, it often resulted in gridlock in OEF, in that it encouraged higher-level leaders and their staffs to try to manage the fighting. Senior leaders often intervened at the tactical level not because circumstances required it, but simply because they could.

A lesson learned from our OEF experience was that expanded global connectivity allowed "reach-back," a desirable capability when used with discrimination, metamorphosed into "reach-forward" as rear headquarters sought information from U.S. Central Command's forward-deployed Combined Air Operations Center (CAOC). Senior HQ then used that information to try to influence events from the rear. Granted, political considerations were so overriding that strict rules-of-engagement enforcement was rightly deemed essential by the Senior Leadership.

Although the nation's command-and-control meshwork has evolved to a point where centralized management of combat has become routinely possible, decentralized and flexible execution remains the core virtue of America's C2 military culture.

Those leaders who saw to the ultimately successful prosecution of OEF were engaged in what turned out to be a fortuitous rehearsal for the subsequent three weeks of major combat against Iraq a year later. Thanks to that, the most nagging frustrations occasioned by America's war in Afghanistan were not encountered, by and large, by those who ran the subsequent war in Iraq. In the latter OIF case, far fewer delays in targeting approvals were encountered, and only rarely did the CAOC have to seek such approvals from higher authority. Moreover, in contrast to the case of OEF, the air component had total control over the daily target list. In the end, the close daily interaction among the most senior leaders, both uniformed and civilian enabled a development of key trust relationships that ultimately gave the CAOC greater execution authority in every respect. All of that proved indispensable in shaping the rapid ouster of Saddam Hussein.[5]

The OEF to OIF evolution is an example of the TTP evolution required and underway as C2 moves into the Net-Centric world. This is the reason why the “Sandbox” exists and why “Sandboxes” share data across COCOM boundaries. Only by actually operating across COCOM boundaries in the “Sandbox” environment will the TTP and required level of trust between senior leadership levels be evolved.

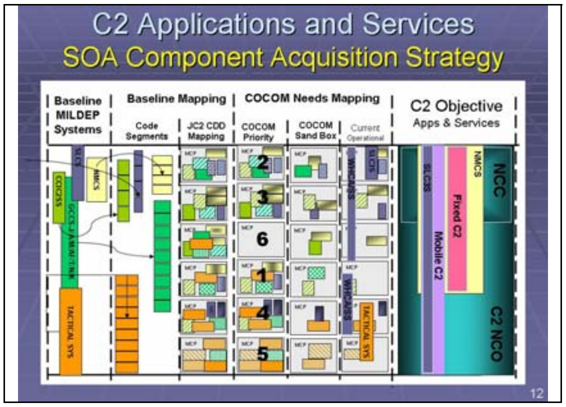
The key to the “Sandbox” is the intimate involvement of the operations staff in testing and certifying the ability of new capability in the Sandbox as meeting their respective military needs. JFCOM, as the force provider, and DISA working together, should maintain COCOM C2 site configuration, while allowing developers to submit new capabilities to the “Sandbox” for evaluation. We deem operator involvement in the evolution of new C2 capability as critical to rapid technology insertion, dynamic reconfiguration and near-term implementation.

C2 Applications and Services (A&S) Component Strategy

As part of the evolution towards acquiring capabilities instead of systems the DoD must also transition from the creation, testing and fielding of systems to the creation, testing and fielding of "components." A component is simply a piece of software and/or hardware that provides an identifiable increment of change in capability.

Much of the software in the existing legacy command and control programs that provide the Military Department (MILDEP) C2 capability are configured as Defense Information Infrastructure (DII) Segments built to operate in the Common Operational Environment (COE).

The previous DISA DII COE effort was a platform based approach, to interoperability that is now being replaced by the Net Centric Enterprise Services (NCES). The DISA DII COE effort forced software developers to break large software applications into DII COE "segments." The Theater Battle Management Command and Control System (TMBCS), for example, consists of more than 70 segments.



C2 Applications and Services
SOA Component Acquisition Strategy

Figure 10

Since many legacy C2 programs are now segmented, this move towards treating software as components provides a baseline upon which to build the future C2 components that will operate within the DoD C2 SOA, see Figure 10. The first step is to baseline MILDEP systems as DII COE Segments.

These segments, now treated as software and hardware components, are mapped to the Joint Command and Control (JC2) Capabilities Development Document (CDD). Figure 10 shows where existing software maps to the JC2 CDD approved by the JROC. Without this mapping, a cost estimate of the "as is" capability of JC2 in terms of today's legacy systems, is impossible.

The world of command and control is constantly evolving to new operational needs and requirements. While the future C2 capabilities of JC2 are expressed in the JROC approved CDD, the order in which those components are acquired, tested and fielded should be based upon careful deliberation between the COCOM's with USJFOCOM participating in its role as Joint Capability Provider serving as the focal point.

We expect this mapping by COCOMs to result in a prioritized list of the JC2 capabilities based on current and projected COCOM needs. We also expect the COCOM forum to determine that parts of the previous mapping of legacy systems to JC2 CDD are inappropriate, given current warfighter prioritization.

To provide an environment in which the COCOMs can use new, rapidly fielded components to co-evolve the DOTMLPF Doctrine, Training and Procedures, we propose the creation of two parallel command center environments at each and every COCOM/JTF location: the operational system and the "Sandbox" as shown in Figure 8, 9 and 10.

This Sandbox-like environment has been used successfully by Google, Ebay, Yahoo and a host of other commercial developments to leverage rapidly changing software environments and promote the use of open-source and alternate procurement methodologies.

We propose that while evolving to the Objective C2 environment depicted on the right side of Figure 10 it will be necessary to have a test, certification and operations environment in which components can be fielded. Whereas the DoD has previously developed, tested and certified systems, one at a time, the change from systems acquisition to capabilities-based acquisition requires an accompanying change in development, certification and testing. The “Sandbox” will provide that distributed environment for integrating C2 capabilities together in new and innovative ways.

We propose that DoD further consider an alternative software procurement methodology. Traditionally DoD has written specifications, OPCON’s and CONOPS in an attempt to describe a needed capability. These documents are difficult to write because they require predicting a future need and then describing the need sufficiently for acquisition purposes.

Since the premise of capabilities-based acquisition directed in DPG 2003 is that we do not know what capabilities we will need in the future and that we need to be able to combine capabilities in new and innovative ways, the current system specification-based approach to C2 procurement will not work in a Net-Centric component based future.

Instead, by posting to appropriately controlled web sites, at the appropriate classification, both the JC2 CDD mapping of C2 capabilities and the current COCOM prioritization, it will be possible for developers, small and large to compete as equals in developing JC2 functionality. This set of developers web sites on each of DoD’s networks will allow all developers to determine how they can provide a JROC-validated C2 capability in the shortest time with existing legacy code, newly developed code or open source utilities.

We propose a future without delay caused by source selections, IPR’s, PDRs, CDRs and delivering a misunderstood capability 5-7 years in the future to end-users. Instead, we propose a commercial model in which developers determine how best to meet the JC2 CDD’s capability needs built in the order of the COCOM’s needs. A capability thus developed would be certified for compatibility with in a Sandbox at DISA, the lead system integrator for DoD C2 and then deployed into the COCOM Sandboxes.

By engaging real COCOM users and interfacing with real data in a controlled environment, software can be both rapidly developed and refined early with constant user involvement into what the COCOM users need now. The current procurement model delivers a capability in 5-7 years that the end-users either cannot use due to miss-understood requirements, or no-longer need due to changes in warfare or TTP.

Only when software has been certified to run in the Sandbox and has evolved to the point that COCOM and other end-users want to field the capability, will it be moved from the COCOM parallel Sandbox to the COCOM operational C2 systems world-wide.

At this point, the end-user has "accepted for use" the software, and DISA, as the system integrator and provider pays for the software/systems. The end-users only pay for software that has already been demonstrated to meet their needs. The risks to the Government and end-users of proposals, source selection and software development as described in the proposal are eliminated.

DoD, in this commercial model, only pays for successful efforts that provide meaningful, near-term C2 capabilities into actual operational use. The expense of "Imagineering"[6] a new C2 capability based upon impossible to predict future conditions and system dependencies gives way to a much more rapid "pay for delivery" paradigm for DoD's C2 enterprise.

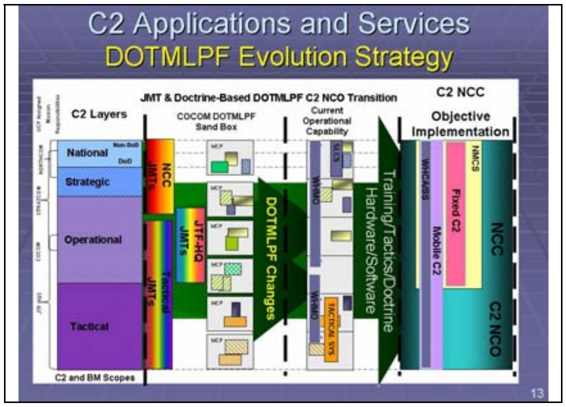
Since approximately half of all software development time for DoD systems is in the specification, RFP and procurement process, cutting this costly part of C2 capabilities development to only the essential "must have" elements will save DoD significant costs on future C2 developments. By not paying until the user is satisfied, by integrating the user early in the development cycle, the costs of development in which the user need was not well understood, could be contained and minimized.

Is doing away with RFP's and source selections controversial? Yes, but it would also enable both small and large industrial concerns to compete fully in the rapid building of creative, innovative solutions in a "Sandbox" to meet DoD's COCOM C2 needs.

The up-front creation of government specifications in this acquisition model is replaced by statements by the current COCOM's of current real-world needs and priorities given the evolution of both the newly fielded C2 system and the evolving TTP. The software developer market is then free to show, not propose, how they will provide the COCOM's near-term C2 capability. The IT environment of today allows and enables the "Sandbox" development environment for DoD.

Enabling DOTMLPF Evolution Using JMT's In The COCOM Sandboxes

Just changing the software and hardware used to support JC2, globally, is not sufficient to carry out the transformation of C2 that is required in the proposed C2 strategy. The evolution to Net-Centric C2 also requires the evolution of TTP, as shown in Figure 11, both from the COCOM down to the JTF execution elements and from COCOMs laterally to each other and upward in command to coordinate activities all the way to POTUS.



C2 Applications and Services

DOTMLPF Evolution Strategy

Figure 11

To evolve the upward portion (COCOM through NMCS to POTUS) of this C2 doctrine without compromising decentralized execution, will require experimentation inside the C2 Net-Centric Sandbox.

All of the information that is available at any COCOM site is redundantly distributed across the global network (GIG). This information availability enables each COCOM to see and coordinate on the details of current and planned operations in a bordering COCOM's Area of Responsibility (AOR) in real-time. The result can be synchronous coordinated operations with complete situational awareness conducted on the AOR boundaries, thus denying our enemies areas of refuge due to lack of timely cross-COCOM coordination.

Additionally, the implementation and fielding of the Missile Defense Agency developed National Missile Defense capability of the United States requires new TTPs to be developed which have not previously existed. Missiles and other ballistic objects in space do not recognize COCOM boundaries. COCOMs must coordinate not only with each other, but with senior national leaders to prioritize and coordinate the employment of national missile defense assets.

This paper proposes a C2 strategy that can provide the necessary DOTMLPF evolutionary capability required by the COCOMs and other senior national leaders to evolve C2 TTPs that have not previously existed. This development will take place in the Sandbox and, as procedures are certified, the Sandbox developed systems and TTP will be moved into the parallel (identical) operational command center.

The JMTs, which are inherently threads of activities, will be used as the operational context and as a forcing function to carry out this DOTMLPF evolution. JFCOM, as the force provider, will document the DOTMLPF changes using the Doctrine Change Request (DCR).

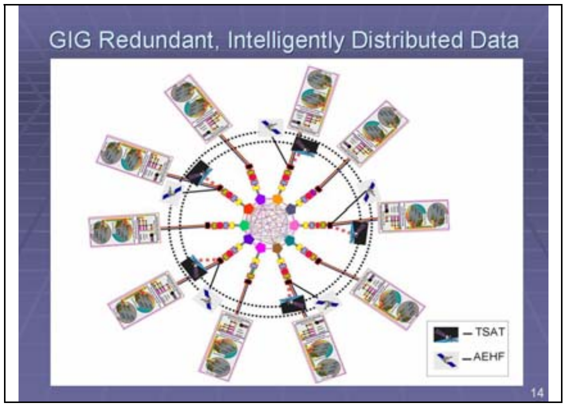
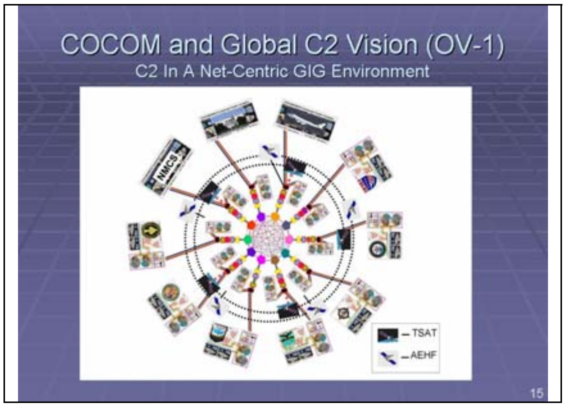

GIG Redundant, Intelligently Distributed Data

Figure 12

Both the COCOM operational system and the "Sandbox" have access to redundant, replicated, distributed, data storage via the three GIG networks shown in Figures 8 and 12. Figure 12 shows the distributed data storage nodes not located at COCOM sites. All stored information available on the GIG is redundant and distributed and available to all users.

Through the use of truly distributed, redundant data storage in nodes throughout the DoD enterprise including at COCOM sites and as part of JTF configurations, the GIG provides authorized users continuous access to all of the DoD C2 environment's data at all times. Intelligent, automated, forward staging of data close to "data consumers" will be used to achieve user acceptable access times.



COCOM and Global C2 Vision (OV-1)

C2 In A Net-Centric GIG Environment

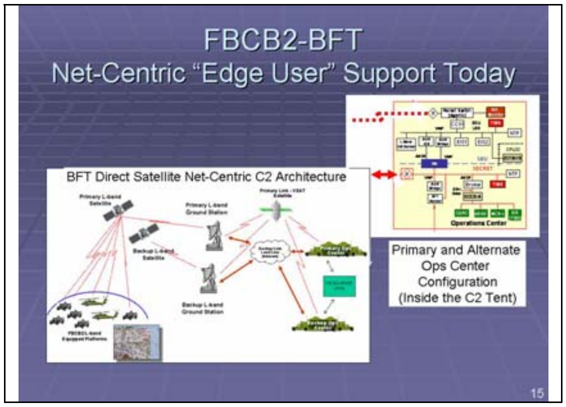
Figure 13

In Figure 13, we show the COCOM command centers from Figure 12 connected to the Global Information Grid (GIG), as standard nodes in the C2 integrating concept. Figure 13 also depicts the physically distributed data storage from Figures 8 and 12 that are not located at COCOM sites.

The GIG enterprise infrastructure must provide the infrastructure transport upon which global information sharing across COCOMs operates. From POTUS to a Blue Force Tracking (BFT) connected HUMVEE, Net-Centric C2 connectivity allows decentralized execution while maintaining uniform situational awareness at all command elements.

The Big Picture – The Enabling Concept Carried To The Edge User

Since many C2 users are by operational necessity mobile, it is essential that no mobile C2 users are "left behind." The rapid development and fielding of a mobile C2 capability formally known as Force 21 Battle Command Brigade and Below - Blue Force Tracking (FBCB2-BFT), and more widely as Blue Force Tracking, Figure 14, provides an example of a mobile C2 capability for Net-Centric users.



FBCB2-BFT

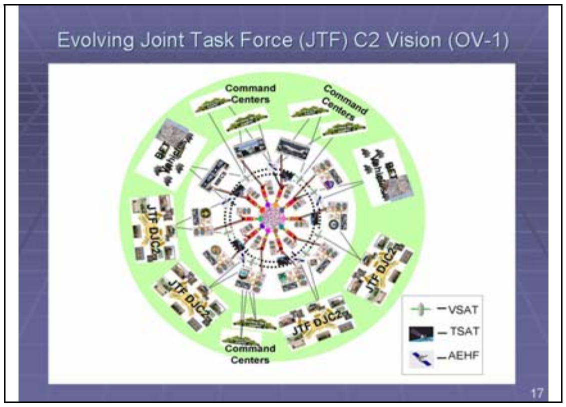
Net-Centric "Edge User" Support Today

BFT Direct Satellite Net-Centric C2 Architecture
Primary L-band Satellite
Primary L-band Ground Station
Primary Link / VSAT Satellite
Backup L-band Satellite
Backup L-band Ground Station
FBCB2 L-band Equipped Platforms
SECRET
Operations Center
Primary and Alternate Ops Center Configuration (Inside the C2 Tent)
15

Figure 14

Tactical users, regardless of location, all require Command and Control support. Force protection principles described in Joint Vision 2020 require that we provide mobile C2 capability "to the edge", the edge of the battlefield where the actual execution of the battle occurs.

FBCB2-BFT provides direct satellite information feeds to combat and non-combat vehicles, and allows forward command posts to coordinate and control force employment and engagement as shown in Figure 14 and 15.



Evolving Joint Task Force (JTF) C2 Vision (OV-1)

Figure 15

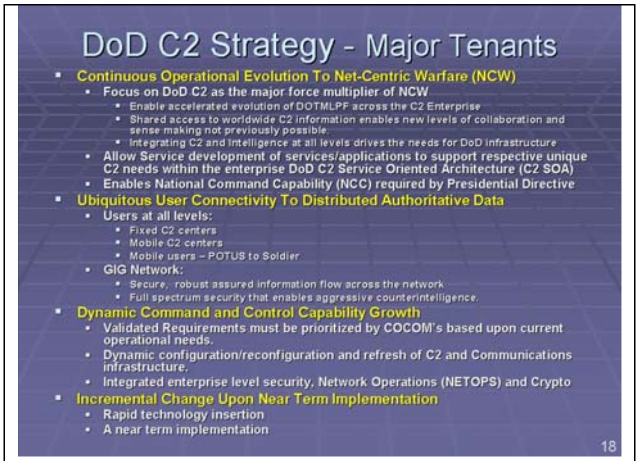
Throughout this paper we have shown the evolution of an enabling pattern-based architecture as part of a C2 strategy. The C2 strategy's enabling network extends from the GIG core infrastructure to the users at the tactical edges. We have shown the evolution of a pattern-based architecture's components consisting of C2 centers, networking and communications nodes, and replicated, redundant data storage nodes that are employed across the GIG enterprise. We have also shown how Command and Control sites, both fixed and mobile can be built up in various sizes using the common patterns of components. The C2 strategy's data center pattern and command and control center patterns evolve within the DoD classified enclave data network pattern worldwide.

The effect of using standard patterns as enabling concepts within this proposal for a DoD Enterprise C2 strategy is to simplify and standardize the evolution of the DoD enterprise. By employing standard patterns it will be possible to integrate enterprise level security, Network Operations (NetOps) and Cryptographic management of the networks and an enterprise-wide user identification process. The resulting enabling network has robust full spectrum security and allows aggressive counterintelligence against the "insider threat."

Conclusion

In Figure 16, we summarize four major tenants of the proposed DoD C2 Strategy. The four major tenants are:

1) Continuous operational evolution to net-centric warfare,
2) Ubiquitous user connectivity to distributed, authoritative data,
3) Dynamic command and control capability growth, and
4) Incremental change built upon a near term implementation.



DoD C2 Strategy - Major Tenants

- Continuous Operational Evolution To Net-Centric Warfare (NCW)
  - Focus on DoD C2 as the major force multiplier of NCW
    - Enable accelerated evolution of DOTMLPF across the C2 Enterprise
    - Shared access to worldwide C2 information enables new levels of collaboration and sense making not previously possible.
    - Integrating C2 and Intelligence at all levels drives the needs for DoD infrastructure
  - Allow Service development of services/applications to support respective unique C2 needs within the enterprise DoD C2 Service Oriented Architecture (C2 SOA)
  - Enables National Command Capability (NCC) required by Presidential Directive
- Ubiquitous User Connectivity To Distributed Authoritative Data
  - Users at all levels:
    - Fixed C2 centers
    - Mobile C2 centers
    - Mobile users – POTUS to Soldier
  - GIG Network:
    - Secure, robust assured information flow across the network
    - Full spectrum security that enables aggressive counterintelligence.
- Dynamic Command and Control Capability Growth
  - Validated Requirements must be prioritized by COCOM's based upon current operational needs.
  - Dynamic configuration/reconfiguration and refresh of C2 and Communications infrastructure.
  - Integrated enterprise level security, Network Operations (NETOPS) and Crypto
- Incremental Change Upon Near Term Implementation
  - Rapid technology insertion
  - A near term implementation

18

Figure 16

To evolve C2 it is necessary that a continuous operational evolution to net-centric warfare take place. We must focus on DoD C2 as the major force multiplier of Net Centric Warfare. This focus will enable accelerated evolution of DOTMLPF changes across the DoD C2 enterprise.

By providing a robust DoD C2 Services Oriented Architecture (SOA) the MILDEPs will be more capable of developing truly unique C2 needs without the expense of duplicative development and sustainment of non-unique software and hardware.

[1] "Sneaker-net": A work around to security or interoperability shortfalls where a C2 user is required to carry portable media from one system to another to achieve the mission. In the operational world floppies moved from system to system and even printing data off one system and then re-typing it into another are examples of "sneaker-net."

[2] Oracle Corporation, "Strategies for SOA success", December 2005.

[3] Donald Rumsfield , Secretary of Defense (SecDef), “The Title “Commander in Chief””, Memorandum U09052/02, 24 October 2002

[4] Director, Joint Staff, “Use of the term: “National Command Authorities””, MCM-0003-02, 11 January 2002

[5].Lambeth, Benjamin S, “Air Power Against Terror: America's Conduct of Operation Enduring Freedom,”, Rand, 2005.

[6] Imagineering was coined by the Walt Disney Corporation to describe the process in which imaginative, creative solution oriented engineering occurs.