Has C2 become an Anachronism on the Net-Centric Battlefield?

By
Alfred V. Newman and Ross W. Wheelwright

Introduction

The evolution of Command and Control (C2) functionality toward Net-Centric Warfare and Net-Centric Operations is already in progress. C2 functionality is not an anachronism of the past, but an integral part of missions across the dynamic battlefields of the past, present and future. We will cite examples that illustrate how C2 already operates today in some areas in a Net-Centric environment and indicate how C2 will continue to evolve as a core Net-Centric capability.

We conclude that the current Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF)[1] approach to developing C2 Systems is, indeed, anachronistic. In the related paper, *A Proposal for a Department of Defense (DoD) C2 Strategy*, CCRP #255, we outline the changes in the development approach necessary to build C2 systems as part of an overall Net-Centric C2 Strategy.

Definition Of Terms

The essence of this paper lies in a common understanding of what we mean by Command and Control and being Net-Centric. The definitions of Command and Control (C2) and Net-Centricity are as widely understood as they need to be. To provide a common understanding of the points to be made in this paper, we provide definitions from authoritative sources for the terms used in this paper below.

"Command and Control (C2) -The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.[2]"

C2 Systems - "Command and Control systems refer to the equipment, facilities and personnel a commander requires to effectively command and control armed forces.[3]"

Net-Centric - Exploitation of advancing technology that moves from an system centric to a data-centric paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.[4]

Net-Centricity - "is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, (Net-Centricity) translates information superiority into combat power by effectively linking

knowledgeable entities in the battlespace.[4]"

Net-Centric Warfare – "and information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence Net-Centric Warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battle space. [5]"

Global Information Grid (GIG) - A globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.[6]

Communities of Interest (CoI) - Collaboration groups 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.[4]

Net-centric Information Environment - Net-Centric information environment utilizes emerging standards and technologies to optimize assured information sharing among all users. It results from implementing GIG component architectures in accordance with the Net-Centric Operational Warfare - Reference Model (NCOW-RM). A net-centric information environment is inclusive of Core and COI enterprise services, and a data sharing strategy that emphasizes metadata concepts, shared information spaces, and the task, post, process, use (TPPU) paradigm.[4]

C2 Joint Mission Threads (JMTs)

The functionality of Command and Control (C2) must be understood in terms of the context in which it is exercised. Many previous studies have discussed the C2 decision process in the context of the Observe, Orient, Decide, Act (OODA), and Monitor, Assess, Process, Execute, Review (MAPER). functional activities for a given mission. In order to discuss Command and Control (C2) functionality in the Net-Centric environment of today, we believe one must make use of the existing command context in which the C2 functionality is expressed in terms of its joint mission and tasks.

The Commander US Joint Forces Command, (USCDRJFCOM), Joint Battle Management C2 (JBMC2) Roadmap document focuses on the C2 operational context by using seven JMTs to facilitate identification of required incremental improvements to JBMC2 capabilities. The JMTs are: Joint Close Air Support (JCAS), Joint Task Force Command and Control (JTFC2), Integrated Air/Missile Defense (IAMD), Joint Ground Maneuver (JGM), Time-Sensitive Target (TST), Joint Fires (JF), and Focused Logistics (FL). For each of these JMTs, the C2 services and applications can be derived from each of the task lists. Recent Joint Capability Area (JCA) guidance from the SECDEF of 6 May 2005 has stated that the JCAs shall be an integral part of the evolving Capabilities Based Planning Process.

The JCAs, accordingly, can be used as a common capabilities language for use across many related DoD activities and processes. As a result, JCAs can be used to develop the core C2 services and applications for each JMT. We will next show how the C2 Service Oriented Architecture (SOA) is fundamental to supporting C2 services and applications.

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.

Because a C2 SOA is based upon loosely coupled C3 services rather than tightly coupled integrations, service oriented infrastructures and applications can change as quickly as C2 needs change. As new C2 processes emerge, existing services can be composed quickly to support these new processes. Accordingly, a C2 SOA is essentially a collection of C2 services (C2 Missions and Tasks). These C2 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. The underlying SOA infrastructure, both communications and information technology, such as Net Centric Enterprise Services (NCES) provides the means of connecting C2 services to each other and growth of C2 capability to the warfighter.

The implementation of the C2 SOA can yield a cost-effective, efficient integration of systems and processes, because it lets organizations 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. One can implement a SOA using any service-based technology, however the emergence of web services technology has provided a powerful new tool set for building loosely coupled services with standard interface definitions.

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, autonomous, stateless computer function that accepts one or more requests and returns one or more responses through a well-defined, standard interface. The details of the actual implementation are hidden behind the interface and are not known to the C2 users. Operationally a user should not have to know the design details of a system to use it to accomplish warfighting missions. 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.

In a C2 SOA, services should not depend on the condition or "state" of any other service. They receive all information needed to provide a response from the request. Given that C2 services are loosely coupled, stateless software, based upon agreed upon data standards and vocabularies, service consumers can sequence them to perform C2 capabilities required by different mission threads.

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. Everyone knows roughly what a "web service" is.[7]

Figure - 1

C2 applications, however, are those "C2 services" that interact directly with the user. C2 applications can be a construct of composable C2 services. C2 applications, as a result, must be tested and developed in a user environment usually called a "Sandbox." It is in the "Sandbox" where the paradigm change must occur in the development of C2 systems. The "Sandbox" is discussed below as an integrating concept.

JCAS C2 Services and Applications

The architecting of a C2 SOA, and in our example cross-JMT C2 services and applications, begins with a decomposition of JMT tasks. Because work is still in progress, we will briefly discuss only JCAS JMT relative to JCAs (tasks) and baseline C2 services and applications in this paper. We intend to develop the broader scope of cross-JMT C2 services and applications later by investigating a selected set of JMTs for each of the command levels of today, National – National C2, Strategic – Global Strike, Operational - JTF HQ and Tactical – JCAS (Figure 1.) We should ultimately be able to articulate common C2 services and applications across these JMTs.

The common, cross-command level C2 Services and applications become the re-usable components for a C2 application, such as targeting. For example, JCAS is a tactical mission application, but is also linked to JTF HQ theater targeting services. Theater targeting is linked to Global strike services, that in turn is linked to National Command and Control services; especially in the case of nuclear strike. One could now derive the common targeting information that must be shared across the associated Targeting applications.

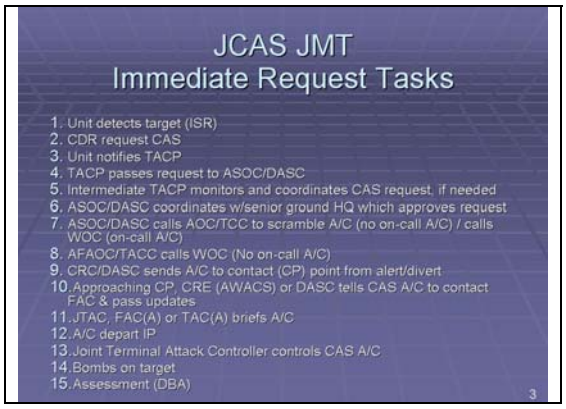

Figure - 2

To begin decomposition of JCAS JMT tasking, we will utilize the JCAS JMT immediate request tasks, Figure 2, to develop the core list of JCAS C2 services and applications.[8] JCAS C2 applications and services typically include C2 functions of joint operations planning, fire support, targeting, surveillance, and bomb damage assessment.

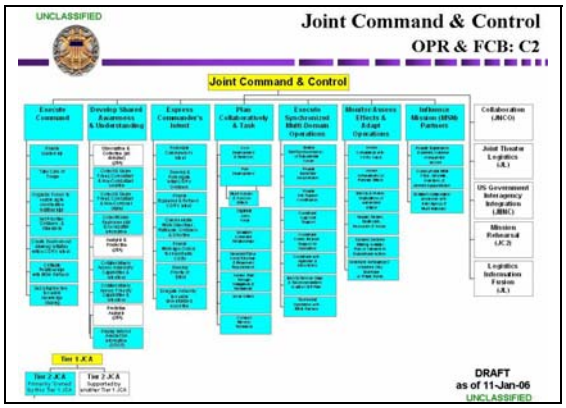

Figure - 3

Since the Joint Staff developed JCAs are intended to provide a common capabilities language, the 15 JCAS *immediate request* tasks are related to the Tier 1 and 2 JCAs for Joint Command and Control (JC2) as shown in Figure 3. JCAS communications tasks can be related to the Net-Centric Operations (NCO) Tier 1 and 2 JCAs. Figure 4 shows a potential set of JC2 services on the three DoD operational networks. Also, note that the JCAS services information in Figure 4 is distributed across the DoD networks by classification. The same C2 SOA exists at each classification level and applications and services themselves are largely common across the three operating environments. The data at each classification level and some functionality will change due to classification.

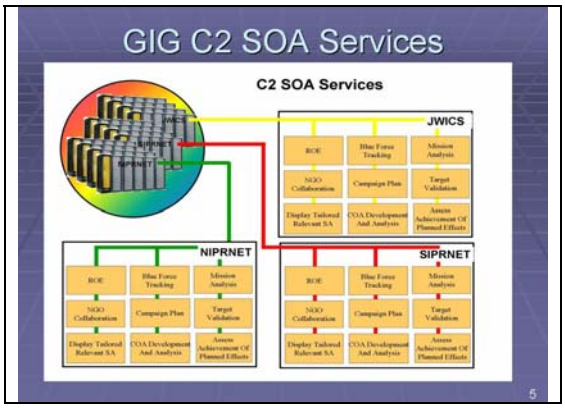

Figure - 4

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

C2, makes use of many sources of information to develop military courses of action in response to threats on the battlefield. Figure 5 provides the notion that C2 dwells in an enclave world of information domains. The C2 function 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 all the integrated information he required to execute his battle plan.

On the other hand, domestically, C2 military functional support to the KATRINA hurricane disaster in New Orleans, Louisiana, moved from the Homeland Security domain to the C2 military domain in Figure 5. Because the JTF commander moved his operation, he had access to all the integrated information he needed, including intelligence information from CNN and a communications infrastructure that worked.

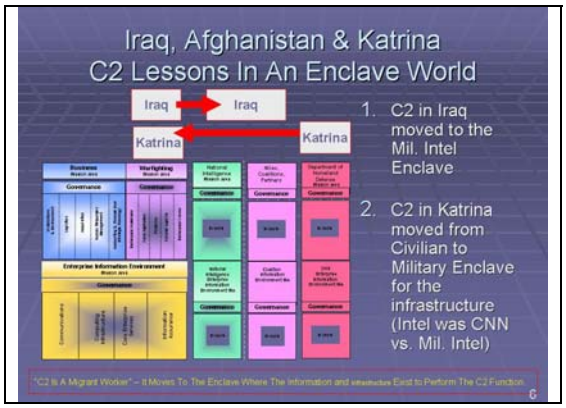

Figure - 5

Because the civilian capability to perform command and control (fire and police actions) in New Orleans was destroyed[9], the DoD military were called upon by the Governor of Louisiana for support and were able to respond by deploying a mobile C2 center, the amphibious ship, IWO JIMA.

Figure - 6

In the domains of C2 and Intelligence, one normally finds that the command nodes consist of both fixed (Figure 6) and mobile nodes (Figure 7) on the GIG network. Some of these C2 nodes are familiar such as, AWACS, White House, Air Force 1 and CENTCOM Headquarters. The C2 command nodes are connected by communications of all types to permit timely information exchange to support senior leadership decision making.

Figure - 7

In fact, the fixed and mobile command centers strongly indicate that C2 exists anywhere that a situationally aware decision is being made or contemplated as seen in Figure 8.

C2 for Continuity Of Operations (COOP) is not a separate facility or backup and restore capability, but exists anywhere, across the world at any time.

Both a person working at a terminal somewhere in the world and a soldier talking on a radio while peering around the corner of a building in Falluja, Iraq, are examples of C2 functions operating within the GIG distributed environment in which the C2 SOA can operates.

The fact that one person has a computer (IT) and the other does not, is not a distinguishing characteristic of C2.

Figure - 8

Figure 9 provides an example of C2 functions operating on the Net-Centric battlefield of today. It shows the operations commander, the pilot of the UAV and the intelligence officer, all working closely together in executing a tactical mission in close coordination with the JTF HQ located thousands of miles away.

Figure 9 also shows that the fusion of operations and intelligence across the OPS-INTEL interface is possible, and can be used today in Net-Centric C2 military actions.

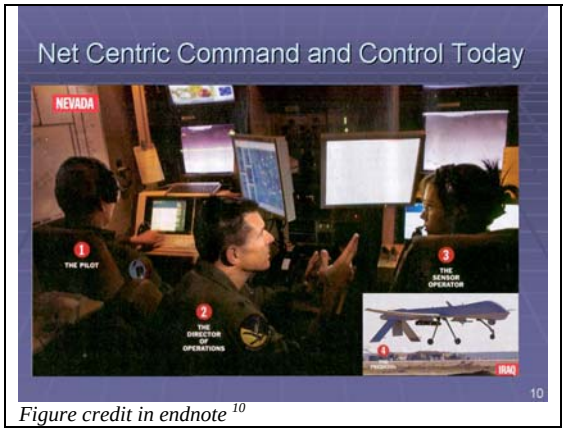

Figure credit in endnote [10]

Figure - 9

Net-Centric C2 is a function in a GIG environment that is networked, distributed, redundant, dynamically reconfigurable, and one in which technology and implementation (Training, Tactics, Procedures) are constantly changing as the battlefield changes.

A C2 SOA allows C2 functionality in the form of services and applications to be available and accessible within this standards based Net-Centric environment. C2 is inextricably connected with intelligence (also identified as an information source in the IT world). This OPS-INTEL information exchange has, historically, been one of the most difficult to achieve in real-world operations.[11]

Again, we ask: "How do you make a C2 system net-centric?" A C2 System is considered net-centric when it is capable of the "exploitation of advancing technology that moves from a system centric to a data-centric[12] paradigm – that is, providing users the ability to access applications and services through services – an information environment comprised of interoperable GIG computing and communication components."

C2 Integrating Concept

In Figure 10 a C2 Combatant Commander (COCOM) command center complex is shown, for discussion purposes, as having two components, the operational command center and a development and test (Sandbox) command center. Both the command center and the development and test center "Sandbox" are supported by common communications infrastructure.

In order to ensure that the future Training, Tactics and Procedures (TTP) development does not degrade into "reach-forward" from "reach-back," the "Sandboxes" must only exchange information with other "Sandboxes" at other COCOM sites and Joint Task Forces (JTF) or with other sanctioned "Sandboxes." The TTP "Sandbox" is required to facilitate the TTP transition of C2 into the world of Net-Centric Warfare.

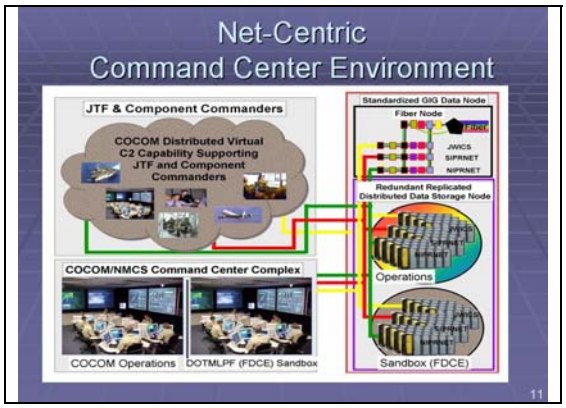

Figure – 10

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 users then used that information to try to influence battlefield events from the rear. Granted political considerations were so overriding at the time 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. In the latter Operation Iraqi Freedom (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 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.[13]

The OEF to OIF experience is an example of TTP evolution required and underway as C2 moves into the Net-Centric world. This operational experience expresses another reason why the "Sandbox" must exist, and why "Sandboxes" must share data across COCOM boundaries. Only by actually operating across COCOM boundaries in the "Sandbox" environment first can the TTP, and required level of trust between senior leadership levels be evolved to the extent possible, prior to operational battlefield conditions.

Both the COCOM Operational system and the "Sandbox" have access to redundant, replicated, distributed, data storage via the three GIG

communications networks shown in Figure 10.

The key to the "Sandbox" is the intimate involvement of the operations staff in testing and certifying of new C2 capability in the "Sandbox" as meeting their military needs. JFCOM, as the force provider, 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 the rapid insertion of technology, dynamic reconfiguration and the near-term implementation of new capability. JFCOM and Defense Information Support Agency (DISA), working together, should use the COCOM "Sandbox" and DISA facilities to permit the rapid insertion of new capability for COCOMs that IT readily allows today.

Figure - 11

In Figure 11, we show the COCOM command centers from Figure 10 in a GIG environment, as standard nodes in the C2 integrating concept.

Figure 11 also shows distributed data storage not located at COCOM sites. All stored information available on the GIG is redundantly distributed and made available to all users. This C2 Data Strategy implementation complies with the DoD Data Strategy, DoD 8320.1, and ensures "need to share" takes precedence over "need to know" as long as security requirements are met.

The GIG network connectivity as an enterprise resource, configured in standardized configurations, connecting to the DoD enterprise components and interacting with them, becomes a standard capability to all C2 users, regardless of geographical location and Range Of Military Operations (ROMO) considerations.

For the same reason, COOP is an integral part of C2 in Net-Centric operations (Figure 8). COOP is built into the core fabric of the C2 Strategy and exists operationally everywhere, at all times. 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.

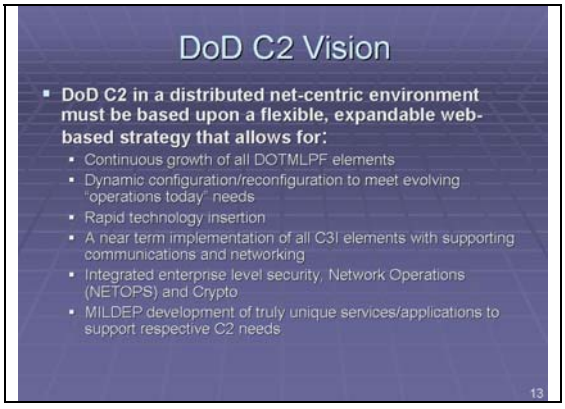

Figure - 12

Conclusion

Figure 12 lists the essential elements of success for evolving DoD's flexible, expandable, web-based C2 strategy. This set of elements can form the basis for the future evolution of Net-Centric C2 in DoD Directives, Instructions, Training, Tactics, Procedures, and Doctrine.

The need for C2 by United States forces has not "gone away" with the arrival of net-centric capabilities and its continued importance today and in the future is underscored by very recent conflicts. As long as senior leaders are precisely aware of the current battlefield situation, decisions can be executed by the on-scene tactical commander with the same battlefield awareness shared by all decision makers world-wide.

We conclude that C2 functionality is not anachronistic on the battlefield today, but the DOTMLPF approach by which C2 systems are developed and acquired is an anachronism.

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.

The C2 capability, built upon a DoD C2 SOA provides the flexible, expandable web-based strategy that IT allows for today: growth, dynamic configuration, rapid technology insertion, and near-term implementation. The C2 SOA enables the Military Departments (MILDEPs) to develop C2 services and applications supporting their own missions and tasks as well as cross-cutting (Joint) C2 services and applications. The development of a DoD C2 strategy whose elements of success are comprised of DOTMLPF, integrated security, Network Operations, Information Assurance (Crypto), all part of Net-Centric Operations, is a daunting challenge.

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. Instead C2 situational awareness and decision-making are facilitated, enabled, and empowered by Net-Centricity thus turning knowledge into combat power.

The challenge is evolving the TTP necessary to effectively enable C2 capabilities to operate in the world of Net-Centric Operations and Warfare.

---

[1] "Joint Warfare Concepts:, 2006, www.dtic.mil/futurejointwarfare/ concepts/jroc_protection_jfc.doc, akss.dau.mil/dag/Guidebook/IG_c5.4.1.asp

[2] "Joint Staff Publication 1-A", http://www.its.bldrdoc.gov/fs-1037/dir-001/_0063.htm#JP1-A

[3] "Army-Technology.com", http://www.army-technology.com/glossary/command-and-control-system.html

[4] Alberts, David S., Garstka, John J., and Stein, Frederick P., Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised), CCRP Publication Series, 1999

[5] IBID, p2

[6] "NII Net-Centric Checklist", May 12, 2005, www.defenselink.mil/nii/org/ cio/doc/NetCentric_Checklist_v2-1-3_May12.doc
[7] Oracle Corporation, "Strategies for SOA success", December 2005.
[8] Joint Staff JP 3-09.3, Joint Tactics, Techniques and Procedures for Close Air Support: JCAS immediate request process
[9] "GAO-06-365R, Preliminary Observations on Hurricane Response", February 1, 2006, http://www.gao.gov/new.items/d06365r.pdf
[10] Picture: "Time Magazine", December 12, 2005, page 42-43
[11] "Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition", http://www.gpoaccess.gov/911/
[12] Data-Centric—focusing on the central design data repository as the foundation or starting point. In a data-centric system, the data is primary and services manipulate the data.
[13] "Air Power Against Terror: America's Conduct of Operation Enduring Freedom," Benjamin S. Lambeth, Rand, 2005