

BUILDING A NETWORK-CENTRIC WARFARE ARCHITECTURE

EXECUTIVE SUMMARY

The United States military is embracing network-centric warfare as it transforms from an industrially oriented Cold War structure to a 21st-century war fighting force. Network-centric warfare is a concept that was derived from analyzing order-of-magnitude improvements in effectiveness by corporations such as Wal-Mart, and law enforcement agencies like the New York City Police Department, through the use of networked information technology. This concept has seen increasing success in the war on terrorism and is changing war fighting doctrine, tactics and force structure in ways not seen since the early days of World War II.

Interoperability, connectivity and network-centric systems are critical elements to field a globally deployed, near-real time force posture. The government is adopting recognized industry standards and creating segmented technology architectures to realize the much higher levels of flexibility, performance, security and connectivity needed in 21st-century systems. The acquisition process itself is changing, because of the clear need to deploy systems now and refine as they are used, rather than taking years to define requirements and build and test an operational system.

The Global War on Terrorism is forcing the United States and its coalition partners to engage a shadowy enemy who does not fight with conventional or symmetric tactics. The way to win is to get inside the enemy's decision cycle, and the way to do that is to have and use relevant information to strike the enemy before he can strike us.

Oracle Corporation has been a leader in helping corporations build global, network-centric enterprises to compete effectively in the 21st century, and stands ready to address many of the challenges that the military faces in transforming to an information-based war fighting infrastructure.

INTRODUCTION

Secretary of Defense Donald Rumsfeld has been driving the United States military to transform itself from a post-Cold War fighting force to one that is capable of addressing emerging 21st-century challenges. A key part of this transformation is leveraging "network-centric warfare", or the synergies derived from interoperable, connected information systems.

We've seen a glimpse of what is possible during the recent Afghanistan and Iraq campaigns, for example, when American special forces soldiers were on the ground—on horseback—using laptops or PDAs to send latitude/longitude information to orbiting aircraft, which then launched precision-guided munitions to defeat Taliban armor and artillery. This example of network-centric warfare enabled the United States to defeat the ruling regime of a country that was perceived to be unconquerable—with less than one-tenth the force structure required in Desert Storm—in less than two months. Armored forces racing toward Baghdad in Operation Iraqi Freedom used network-centric capabilities to monitor the battlefield situation during horrendous weather conditions to accomplish the most rapid military advance in history and to overthrow Saddam Hussein's regime in a matter of weeks.

This paper addresses the challenges faced by the military to build an effective network-centric warfare infrastructure and Oracle's response: a network-centric warfare architecture.

WHAT IS NETWORK-CENTRIC WARFARE?

Network-centric warfare is the term used in military circles to define information-based warfighting. Systems are interconnected in near-real time, and provide order-of-magnitude improvements in the ability to bring commander's intent and overwhelming force to the enemy at precise points—without the logistics tail that had been required in earlier stages of warfare.

Network-centric warfare is staged in a battle space, the three-dimensional extension of the traditional battlefield. Of paramount importance is the availability of accurate, relevant and timely data throughout a globally aware infrastructure—a common operational picture. Sensors, platforms and operators (military forces) are all connected to share information. Forward-deployed forces can use “reachback” to get information from intelligence databases located in the United States. Air, ground and sea forces can “self-synchronize”, or rapidly tailor their capabilities in new ways to address emerging combat situations. As will be explained more fully below, network-centric warfare does not eliminate the decision-making authority of the front-line combatant in favor of centralized command and control, it rather enhances the ability of the individual combat unit to see the big picture, draw on available resources, and reduce the “fog of war”.

As in the business world, the effects of information technology on 21st century war fighting are revolutionary and far-reaching. War planners and strategists have been predicting radical change based on technology for some time. The current issues facing the military are how to best use information technology, how should the military's 21st century information technology infrastructure be built, and how will forces organize to make the most use of information technology while preserving the traditional “boots on the ground” advantages of forward persistence and presence.

The Global War on Terrorism: Asymmetric Warfare in the 21st Century

As the Global War on Terrorism continues, the United States and its coalition partners are increasingly faced with the difficult task of engaging a shadowy enemy who uses asymmetric force against us from anywhere in the world.

Combatant commanders have less time to mass forces or anticipate symmetric force-on-force battles the way previous generations prepared for the wars of the 19th and 20th centuries. Now, the coalition must maintain a *sustained global presence* and be able to strike literally within minutes to respond to or preempt a threat.

Terrorists, as small groups or even individuals, are constantly seeking new ways to inflict serious damage against our forces—and our homeland—by coming out of the shadows to strike against our weak points. The challenge before the 21st century military is to find and pre-empt the terrorists before they are able to strike, i.e., to get inside their decision cycle. The military uses the term “OODA Loop” to define the decision cycle. OODA stands for Observe, Orient, Decide and Act. By being able to get inside the enemy's OODA Loop, we can gain the advantage and protect American citizens and property.

The military is beginning to realize the power of finding and sharing relevant information and using it in a timely manner to keep our enemy off balance. Threats, targets, intelligence analysis, logistics information, and personnel data can now be weaved together to paint that common operational picture and allow the theater commander to prioritize missions much more rapidly than before. General John Jumper, the Air Force Chief of Staff, talks about a “ten-minute kill chain”, essentially being able to target and eliminate a threat within ten minutes of its appearance in the battlespace.

Coalition forces make up a very important part of the Global War on Terrorism. As countries decide to support specific operations and enter into the coalition, the need to share certain pieces of information while withholding others becomes paramount. The theater commander must have information systems that can recognize sensitive information and the users who need it in a flexible yet secure way.

As the military begins to realize the vision of a standardized network-centric infrastructure, more and more flexible and dynamic ways to engage the enemy will emerge. Operations Enduring Freedom and Iraqi Freedom are analogous to

Lieutenant Colonel Eisenhower’s trip across the country in a military convoy. It could be done, but in the future it could be done a lot easier, and there was a fundamental transformation of the American military and culture along the way. Similarly, the story around NCW is just beginning!

Network-Centric Warfare Visualized: Building the Common Operational Picture

The top third of the following picture shows the many different systems, platforms and forces that must connect to a network-centric warfare architecture, and the requirements for operating it, i.e, security, global deployment and communications and data management. The “system of systems” connects and interoperates to form the important “common operational picture”, which is represented in the middle of the picture. Forward-deployed air, sea or ground tactical operations centers can view the same information and combine resources for rapid-targeting of enemy forces, or shape the information presentation to their own needs. Rear echelon command centers monitor the same information to address evolving needs. The bottom third of the picture highlights several technology features that enable the network-centric warfare infrastructure. Each will be discussed in more detail in the sections below.

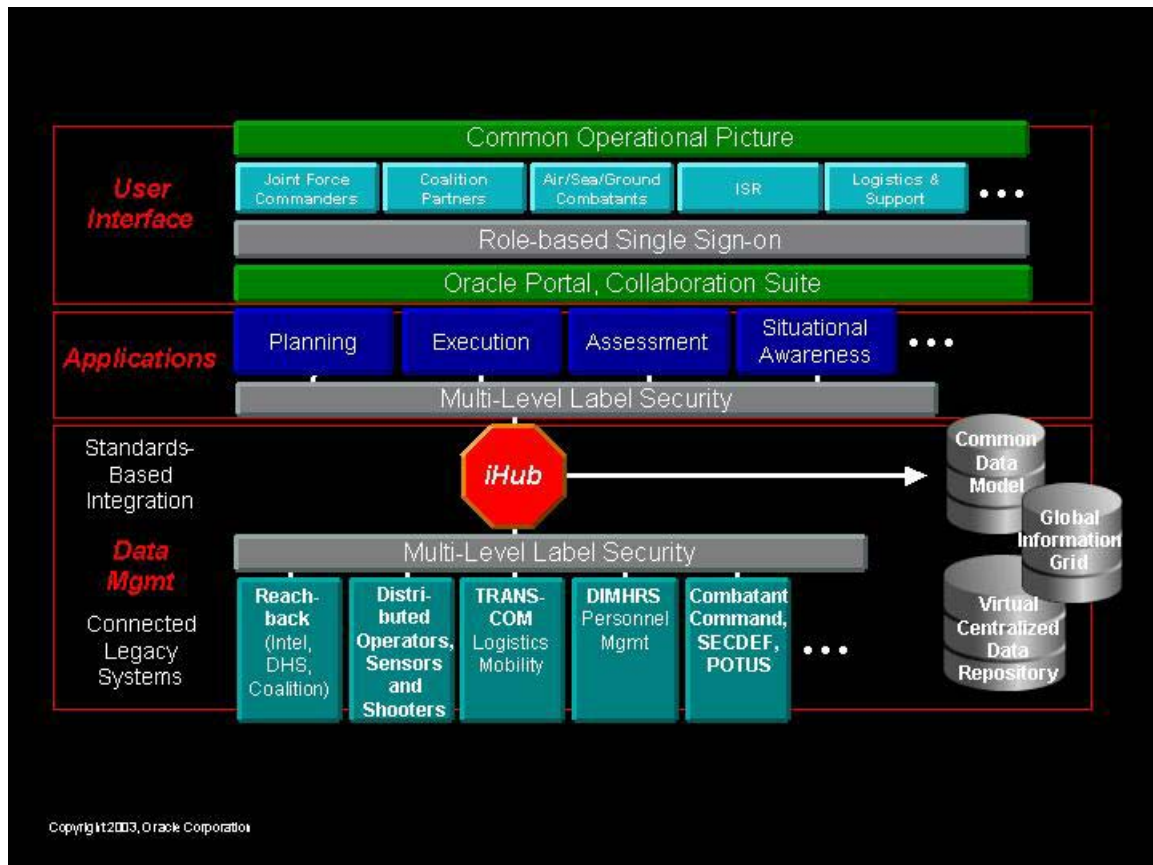


ORACLE’S NETWORK-CENTRIC WARFARE REFERENCE ARCHITECTURE

Admiral Cebrowski and John Garstka derived the network-centric warfare concept from their observations of commercial companies that used information technology to gain major competitive advantage. Oracle Corporation is a network-centric company with offices in over 100 countries that all work from one global data infrastructure. That means tremendous economies of scale in terms of managing the huge amounts of information that flow within and outside the company’s enterprise boundaries on a daily basis. Every Oracle employee anywhere in the world can

access the same information, and resources can be brought to bear much more quickly to address rapidly evolving business situations.

The following picture shows Oracle's approach to building a global, network-centric warfare architecture.



Implied in this picture are three levels of system interaction: The user level, the application level and the data level. When a systems architecture is built in these three segmented levels, it introduces a very high degree of flexibility in terms of managing the overall system and evolving new capabilities.

ORACLE ARCHITECTURAL SOLUTIONS:

Multi-Level Data Security

Security is managed in a network-centric environment by providing “identity management” capabilities, i.e., directory-based access to users, networks, services and other systems, and granular labeling of data. Therefore, if a user, service, network or system wishes to access data, it must establish a profile of authorized access levels, and the enterprise can grant or limit access to data and even to search capabilities. Oracle provides granular data element-level security classifications to create a very rigorous, yet flexible and maintainable multi-level security capability.

Legacy Systems Integration

The challenge most enterprises face today is that they have a hodgepodge of stovepiped legacy systems built on different architectures and data models. Interoperability is achieved only through a complicated “spaghetti” maze of point-to-point integrations, or through some type of hub and spoke enterprise application integration (EAI) model.

Fusion of information from different sources is typically done manually or through a series of applications that are tailored to solving one particular kind of problem.

Oracle uses an “iHub” to facilitate integration of disparate legacy systems, messaging standards and translated data models. This message-based, workflow-enabled integration hub provides a wide range of integration capabilities in a manageable format. Legacy applications can communicate directly with the hub, and new applications can be built using the segmented architecture to focus on business logic rather than integration. Applications are abstracted by the hub from the data and user layers, which minimizes the impact on the rest of the infrastructure when they are retired, replaced or modified.

Community of Interest Data Sharing

As the computing industry matures and enterprises evolve to common architectures and services, integration of disparate systems will become much less prevalent. By building a common enterprise data model and locating all of the services management and development frameworks at the data level, companies will be able to utilize a far greater set of compliant applications, users or registered services to meet their business needs. The data layer is not expected to change frequently, and is meant to be the foundation of the overall enterprise architecture. Over time, as more systems are migrated to new network-centric architectures, and network-centric enterprise services are used more often, there will be an “economic” push to create community-of-interest semantics in a common data infrastructure.

Geo-Spatial Data Representation

A critical element of establishing the common operational picture is the ability to represent data in geographic terms, such as force structure and threats arrayed on a map. This helps the commander, war fighting forces, intelligence analysts and logistics providers to synchronize and respond to events in much shorter timeframes. In a network-centric information infrastructure, geographic imagery is referenced to predefined spatial coordinate systems to provide accurate targeting and intelligence analysis capabilities. Oracle 10g Spatial provides high-performance, secure georeferenced raster imagery, XML schema and flexible geocoding inside the database.

Global Data Management

Eventually, the military, and the federal government, will operate from very similar standards-based information architectures. Network-centric operations will be conducted over a global infrastructure where network-enabled platforms will register as “services” via the Global Information Grid and be able to interoperate as nodes, platforms and services in a highly connected environment. The assembly of all of these physically distributed, interconnected nodes will create a *virtual global information infrastructure* that enables the reachback, speed of command and self-synchronization abilities envisioned for network-centric warfare. Oracle has very strong experience in building global information infrastructures, and saved over a billion dollars a year in internal operating expenses by moving to an internal “single global instance” infrastructure. Oracle’s products contain a variety of features designed to operate high-performance, highly available global information technology infrastructures.

Complex Analysis and Data Fusion

Network-centric warfare will be conducted by taking in multiple sources of data and fusing them to create the common operational picture. Much of this information will be location-based sensor data that must be tied to intelligence information and the reports from fighting units involved in tactical engagements. Systems that provide high transaction rates, complex analysis tools and effective means of presentation to different types of users are of critical importance in this environment. Oracle provides a wealth of sophisticated data analysis tools, the high performance 10g data

infrastructure to manage the transaction rates for information collection, analysis and dissemination, and the 10g and Collaboration Suite platforms to manage the presentation of the analyzed information.

Rapid, Adaptive Development

Applications developed during the Cold War, be they mainframe or client-server or even early web-based ones, typically were self-contained and highly stovepiped. Any modifications to the application would typically introduce errors that made overall system management and support a very difficult task. As computing standards evolve and mature, the ability increases to create libraries of reusable business objects, publish and orchestrate web services, and to sequence workflow elements to execute evolving business process flows. This provides a much more robust application development environment, because much of the “plumbing” of security, presentation, data management and integration are handled in standardized frameworks.

Segmenting business logic from data and user logic allows for much more flexibility in developing applications, and drives up quality very significantly. Because development cycle times go down and quality goes up, new features can be brought on line much more quickly and less painfully than before. This allows for a higher degree of “operational experimentation”, i.e., testing experimental applications, features and workflow sequences in an operational environment without taxing that environment too heavily. Also, emerging requirements can be addressed in much shorter timeframes for much lower costs. Application development becomes much like an assembly line, just pick the business logic “parts” out of the library and assemble them in the way that fits your current needs.

Oracle has a very robust set of development tools and frameworks in its 10g application server. These J2EE tools use the Model View Controller Framework, which is based on the Unified Modeling Language and is designed to operate in the segmented architecture discussed here. It promotes iterative, spiral development, rapid deployment and reconfiguration, and high levels of component reuse.

Collaboration

Network-centric warfare requires a high degree of collaboration over a robust technology infrastructure. Real-time target planning, intelligence sharing, “self-synchronization” and the ability to get inside the enemy’s decision loop all require users in different locations to be able to share information simultaneously. Oracle Collaboration Suite provides electronic chat rooms, virtual whiteboards and the ability to manage voice, video and data.

Configurable User Interfaces

In the past, each application had a built-in user interface, which required higher levels of maintenance and training because each one was different. With the rise of the World-Wide Web, organizations put “front ends” on their applications to allow people to access them over the web. Portlets then became prevalent, and allowed for dynamic rendering of information based on user actions or other contextual information.

As information technology architectures mature, the user interface becomes even more separated from the underlying application, yet is based on standardized protocols. User interfaces take on the form of web pages, voice, wireless and aircraft cockpit displays. The user interface is very flexible and configurable, basically to the mission requirements and personal tastes of the end user. Oracle 10g provides highly configurable user interface capabilities with the Portal, single-sign on identity management and Lightweight Directory Access Protocol, portlet design and repository management, and wireless access.

Solution Architecture Engineering

As information technology infrastructure becomes more critical to war fighting systems, the dependence on those with expert knowledge of networked business architectures increases. General John Jumper declared the Air Operations

Center a weapon system, and the commander of the Eighth Air Force stated that his relief would most likely be an information operator rather than a pilot. The military must realize that its investment in weapon-class information systems will only be optimized if it also invests in the best engineering talent to maintain them.

Oracle Consulting is an organization of highly trained architectural experts on Oracle technology. They have broad experience in the enterprise view of technology infrastructure, and employ mature and proven standards-based frameworks to manage network-centric infrastructures. Oracle Consulting paved the way in the commercial world for drastically reduced enterprise system implementation times, and has leveraged the Internet for training, operations, worldwide development and technical support. Oracle Consulting's focus is on speed, value and simplicity—critical attributes in the network-centric world.

CONCLUSION

The U. S. military is undergoing its most extensive transformation since before World War II, and is rapidly evolving from an industrial-based Cold War model to a 21st-century information-based war fighting force. Network-centric warfare is emerging as the guiding paradigm for driving this transformation and, in a reversal of roles from previous transformations, is drawing its guidance from the commercial business world. In that world, market and product lifecycles are measured in months, and change is the operative norm. Physical assets are less important than the intelligent use of *knowledge*. Companies with technology infrastructures and business practices that help them get inside the decision cycle of their competitors are at a decided advantage.

In the same way, the military has realized the need to transform as the nature of threats to the nation have dramatically changed from the symmetric Cold War face-off against the Soviet Union. The military leadership is committed to the change, as the ability to stay inside the enemy's OODA loop becomes even more important in the shadowy asymmetric warfare being fought by terrorists and rogue nations.

Oracle is a network-centric company that has the technology and experience to assist the military in its transformation. Oracle's 10g Database and Application Server, Collaboration Suite and e-Business Suite are all products that can be used by the military in network-centric weapon systems. Oracle Consulting provides the engineering expertise to implement, maintain and evolve these network-centric systems to meet the emerging threats of the 21st century.

Copyright © 2004, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.