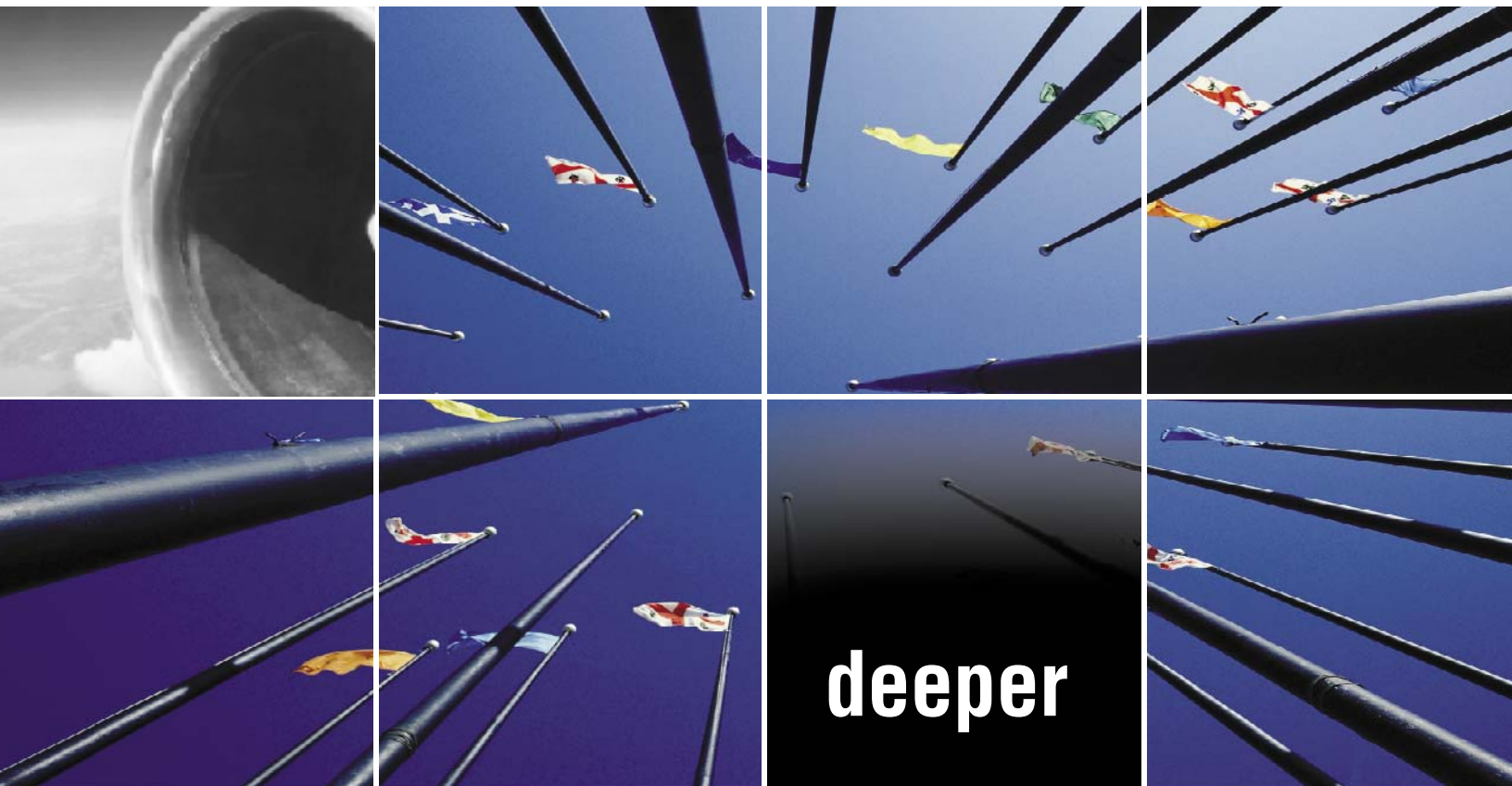


Network-centric operations

The key to military transformation in the 21st century



An IBM Institute for Business Value executive brief

The IBM Institute for Business Value develops fact-based strategic insights for senior business executives around critical industry-specific and cross-industry issues. This executive brief is based on an in-depth study created by the IBM Institute for Business Value. This research is a part of an ongoing commitment by IBM Business Consulting Services to provide analysis and viewpoints that help companies realize business value. You may contact the authors or send an e-mail to iibv@us.ibm.com for more information.

Contents

- 1** Executive summary
- 3** Introduction
- 4** What drives the military toward network-centric operations?
- 5** What does the network-centric military enterprise look like?
- 8** What are the key capabilities of a network-centric military enterprise?
- 10** What are the key issues to address?
- 11** The transformation process toward 21st century operations
- 15** Supporting role of the defense industry
- 17** Conclusion
- 18** Contacts
- 19** About IBM Business Consulting Services
- 20** References
- 21** Bibliography

Executive summary

This white paper presents a high-level view of network-centric operations for the military. It discusses transformation of the armed forces from the current platform-centric organization to a network-centric organization, which it is anticipated will increase effectiveness exponentially.

The broader concept of network-centric operations is explained. It is important to realize that the network-centric operations approach is not just a technical realization. It requires changes in human and organizational behavior as well.

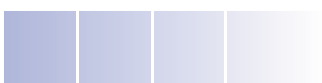
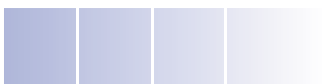
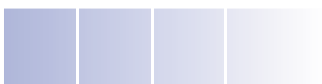
The most important drivers for this transformation are described. Some of these drivers are military specific (e.g., avoiding friendly fire), while others exist in commercial industries as well (e.g., the technological enablers in the mobile domain).

The organization of armed forces that are network-centric-operations enabled is illustrated. This organization is depicted not from a structural, departmental or process view, but from an operational view. Networking the organization puts more stress on the organization's structural flexibility and processes to enable quick response to asymmetrical, unexpected events.

The key capabilities of a network-centric military enterprise are threefold: agility/adaptability, scalability and interoperability. To enable these capabilities, they need to be integrated across people (e.g., training, education), organization (e.g., structure, doctrines) and systems (e.g., requirements for new acquisitions as well as upgrading legacy systems). Although this seems simple, it requires a drastic change of thinking for an organization that traditionally has thought and acted in a "stovepiped" way.

Turning the vision to reality requires addressing a number of issues:

- Resilience is of utmost importance.
- Given the need for interoperability for joined and combined missions, the use of commercial-off-the-shelf software (COTS) is emphasized more than in the past. At the same time, the military-specific requirements place high stress on the capabilities of COTS software.



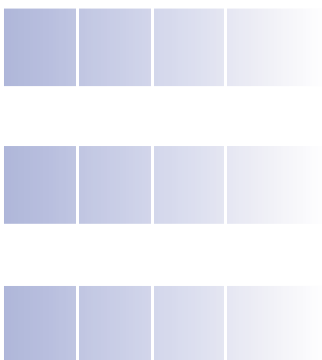
- Security is a domain that needs a client-specific approach. A balanced approach is necessary to maintain the optimum balance between protection of information and availability of information.
- Trusted relationships and partnerships are a basic cornerstone to achieving success. Network-centric operations will operate within the armed forces, between different armed forces, and between the armed forces and their partners. Only if those three levels are truly networked can one can reap the full benefits.

Progress will begin through small steps. A roadmap to evolve to a network centric enabled state starts with the vision. The first implementations on the field are relatively small, but very promising. The recommended approach to take to move to network-centric operations is based on two main principles:

- *Start small and think evolutionary* – Pay the “entry fee” of networking the military enterprise.
- *Work in incremental steps* – Experiment and gradually add functionality while at the same time optimizing the underlying processes.

This paper also highlights the supporting role the defense industry plays. Private industry can bring its lessons learned to the table. This is true especially in connection with e-business, which has been hyped in the past but is now downscaled to what is feasible and proven. The experience gained by the commercial industry during large-scale transformational implementations can benefit the armed forces in their practical realization of network-centric operations.

Because of the complexity of all-encompassing transformation to network-centric operations, the armed forces will need partners on which they can rely. The armed forces also need to procure the services of partners who reward innovation, even if it includes temporary failures. Progress can only be made when new ground is broken.¹



Introduction

Traditionally, military organizations have focused primarily on delivering military mass and power into the battle space. This approach to military operations has been platform-based, but that is now changing in military organizations around the world as they move toward network-centric operations.

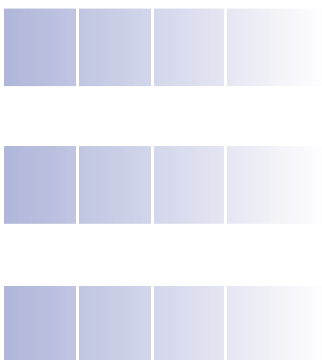
While the details of new network-centric operational concepts being applied by different nations vary, the new concepts are all underpinned by the common understanding of the changing and growing role that one critical factor will play in increasing military effectiveness: information.

The intelligent use of information across an organization and its partners affects and influences all aspects of that organization – from the front line to the back office, from equipment purchase to financial controls, and including the organizations' relationships with its partners, whether they are commercial suppliers or other government organizations.

Based on the experience to date of existing defense initiatives in this area and similar experience from the commercial sector, a growing body of evidence shows that these initiatives succeed only where the focus is on the co-evolution of people, doctrine and organization rather than this being seen as a by-product.

Network-centric operations is an approach to the conduct of military operations that derives its power from human and organizational behavior changes and innovative changes to the conduct of warfare that can be enabled by networking.² Network-centric warfare is about human and organizational behavior.³

For network-centric operations, the purchase and deployment of net-ready equipment and systems alone will deliver little benefit if the processes and procedures that govern how they are used are left unchanged. Another key challenge in achieving success will come from prioritizing and coordinating the myriad pieces that make up these initiatives. Coordination across equipment and system programs alone is insufficient. Success will be realized only if the approach and the changes it requires are embedded across the whole organization – in the way its people think, train and act and in everything it does.



The most effective organizations' strategy to ensure their ability to respond quickly to any demand, opportunity or external threat places information at the center of the organization. The process of achieving this goal is termed *IT enabled transformation*. This is an approach that has been used to great effect in commercial and public sector organizations.

This paper presents a vision of how corporate transformational processes can be applied to military organizations to help address the opportunities and issues presented by network-centric operations. A summary of the key drivers for these initiatives and the results they are trying to achieve is included. This paper discusses:

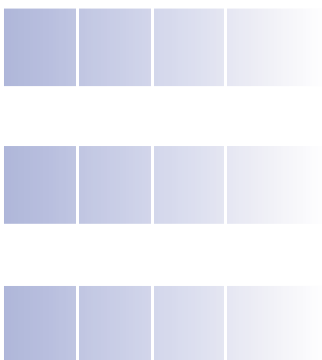
- How a transformational-based evolutionary approach can help ensure delivery of these benefits within the complex world of defense
- How the private sector can bring its capabilities to bear to assist in their delivery.

What drives the military toward network-centric operations?

Strong worldwide interest in the transformation of armed forces toward 21st century operational concepts was sparked by the 1999 book, "Network Centric Warfare", by David S. Alberts, John J. Garstka and Frederick P. Stein.⁴ This book describes the network-centric warfare concept, identifies the challenges in transforming the concept into a real operational capability and suggests approaches to meet those challenges.

In addition, the following drivers have become more conspicuous and are contributing to the need for modern armed forces to begin focusing on network-centric operations:

- The range and scope of military operations are increasing. A single military organization can expect to be involved in multiple simultaneous operations ranging from humanitarian aid to peace enforcement, spread across the globe. This requires adaptable and agile forces that can deploy rapidly to take on a range of operational tasks.
- Military operations now are rarely carried out by a single country's forces. Operations are carried out in ever-changing coalitions. For effective operations, these dynamic coalitions need to operate as a seamless single entity.



New approaches to command and new command arrangements are needed to effectively flatten hierarchies, free information flow (not orders) from the chain of command, and enable the enterprise to increase the speed of command to lock out adversarial options and achieve option dominance.

Network Centric Warfare,
David S. Alberts, John J. Garstka,
and Frederick P. Stein.

- The demand for information from both politicians and the press is increasing. The military organization needs to provide accurate and timely information because everything that occurs on a military operation now is in the public spotlight.
- The need to avoid fratricide (also known as "killed by friendly fire") and collateral damage is greater than ever before, which reinforces the need to share and collaborate on joint operations.
- The economics of information has changed. Many private sector organizations are connected to a mobile workforce. The technology that enables this – albeit more complex due to military issues such as security and assurance – can now be applied to a military context to improve the effectiveness of a mobile operation.

What does the network-centric military enterprise look like?

In response to the drivers mentioned by Alberts, et al, many military organizations worldwide are taking steps to become more network-centric. In taking these steps, organizations need to think of themselves in terms that describe their operational and information needs rather than their formal structure. They also need to describe their objectives in terms of the capabilities they wish to have rather than as specific technology aims when addressing the drivers. The following discussion illustrates a way of describing a military organization in terms of its information needs and the capabilities it wants to achieve.

An operations-based organizational structure

To understand how to apply network-based concepts to a military organization, that organization needs to be described in a way that shows its operational and information needs. Figure 1 provides an example.

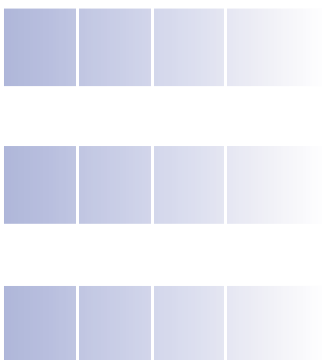
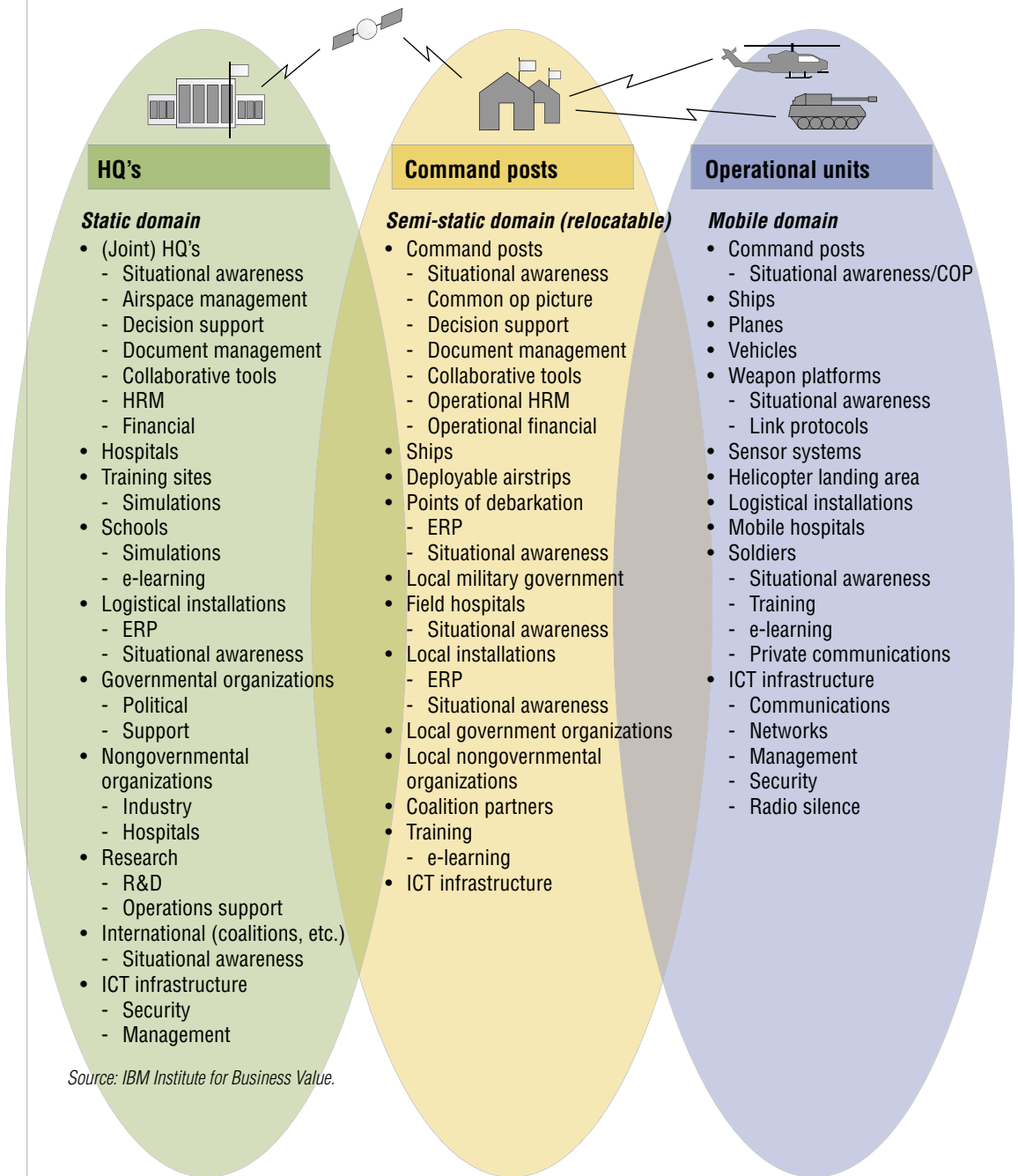
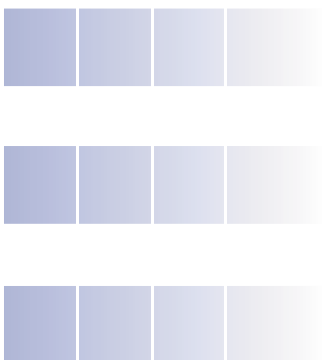


Figure 1. Integrated three domains of the military environment, as part of the envisioned end state.



Source: IBM Institute for Business Value.



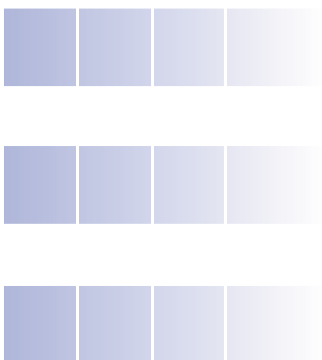
The enterprise shown in Figure 1 is composed of three strongly integrated domains:

- *Static domain* – Includes homeland facilities and all supporting processes among organizations that are part of the defense enterprise
- *Semi-static domain* – Consists of the headquarters of the combined joint task forces, ships, deployable airstrips, etc.
- *Mobile domain* – Supports actions in the full spectrum of operations, where timing is highly critical.

This network-centric defense enterprise will be networked on many levels: the physical network level, the application and information level, and the business process level. The ultimate goal is for all efforts in the three networked domains to focus on support of operations in the mobile domain and their operational effectiveness.

For the mobile domain, networking capability on the physical level entails a self-configuring mobile infrastructure that supports the various services, like video, audio and data exchange. Mobility of individuals, command posts, units, sensors and shooters is supported virtually seamlessly and transparently. Defects and related maintenance of the network are reduced through its self-healing characteristics. Wireless communication extends the reach of the network down to the single soldier in a fully security-enhanced manner. Security is implemented transparently; single sign-on is based on biometric characteristics. Batteries and other physical means help keep the infrastructure up and running under the most severe circumstances, for weeks at a time, without needing a replacement. Seamless connectivity with the other domains is supported, and existing bandwidth limits are managed dynamically. Processes, organizational structures and tactics are adapted organically to the changing operational environment.

On the information level, an integrated system is designed to provide information in every format on demand to every device, responding to dynamic information needs in the operational domain. Multimedia information is integrated via one portal, configurable for each user and each device. Interoperability is implemented throughout the enterprise. All relevant and required information from the whole enterprise can be made available on a realtime basis in the operational domain. Information enrichment and analysis is done partly by machine intelligence and partly by humans, with the balance between them managed dynamically.



At the *cognitive and social level*, operational processes, organizational forms and tactics are adapted organically to the changing security environment. Based on operational events and the need to act on them most effectively, collaboration can be rapidly created between relevant stakeholders throughout the military enterprise.

Information dominance is achieved through effective exploitation of the high availability of information. Leadership states clear examples of collaborative behavior in the network, stimulates sharing of information and creates an environment in which innovation and learning flourish.

Aspects of trust are essential at the social level. Sharing information, e.g., publishing information in a broad networked environment is based on mutual trust between the people in the network.

What are the key capabilities of a network-centric military enterprise?

The co-evolution of technology, informational and organizational change discussed can deliver a substantially more effective military organization with the capabilities of agility, adaptability, scalability and interoperability.

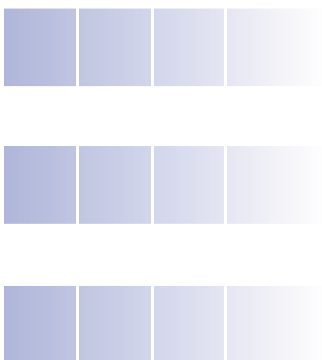
Agile to deliver rapid and dynamic response capability and adaptable to deal with change

The new strategic environment requires agility. Military organizations need to deliver:

- Rapidly mission-ready units
- Units capable of conducting operations in the full mission spectrum worldwide
- Units capable of adapting to changing security and operational environments (e.g., the change from peace enforcement to peace support).

In the early indicators of the lessons learned during the Iraqi operations, it is recognized that to achieve "high" agility, the different branches of the Service will increasingly depend on each other. Therefore, joint and combined training will be promoted more during peacetime to forge even stronger bonds inter-Service during wartime.⁵

Equally important is the need to work alongside other government departments and nongovernmental organizations and to establish arrangements that facilitate the transition to a post-warfighting phase.⁶



To meet these objectives, an enabling technology infrastructure that delivers the right information to the right people at the right time in the right format will be required. In the U.S. operations in Afghanistan, for example, the Predator unmanned aerial surveillance vehicles were armed with Hellfire missiles, thus combining sensors and weapons systems into one package, with the package supported by increasingly accurate and comprehensive information systems. The combination of technologies and at least the limited introduction of network-centric warfare lent new meaning to an old concept of "armed reconnaissance" and provided a new paradigm for technology synergy.⁷ More importantly, it requires an organization structure and command procedures that support rapid decision-making based on that information at the operational unit level.

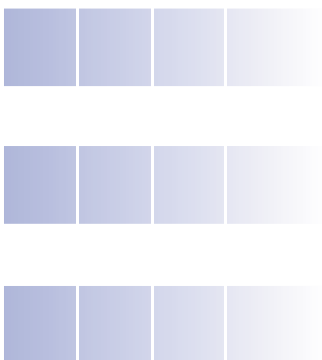
Scalable, both up and down, to deliver flexibility into the operational environment

Scalability is the ability to change the size and reach of the deployed force and its support environment to meet the dynamic needs of the operation. The need for scalability, especially when combined with the complexity of deploying military processes on a large scale, places strong demands on the networked military enterprise. During operations, periods of scaling up are followed by periods of scaling down, with corresponding impacts to the network at any particular point in time: degree of mobility, level of usage and means of communication and whether non-governmental organizations or other allies are involved.

To deliver scalability, the organization requires a flexible approach to networks, systems and coalitions that is designed to flex seamlessly, without negatively impacting military effectiveness. This has both technology and organizational impacts.

From the technology perspective in the highly mobile domain of military field operations, the combination of scalability and complexity necessitates a balanced approach. For example, in any given situation, leaders may have to choose between functionality and limited bandwidth or between autonomy and limited maintenance.

From an organizational perspective, a view of the organization that includes other nongovernmental organizations is required. For example, at a certain phase of an operation, the capability to incorporate local suppliers in the military networked enterprise is crucial for the successful fulfillment of an operation.



Interoperable on all levels to help ensure effective collation operation

Interoperability is the seamless integration at the information, social and cultural levels both within a single country's military organization, between the different organizations within a single country (e.g., the homeland security forces and the armed forces) and between members of a coalition.

At a technical level, communication and data exchange standards and common security protocols are required to allow free exchange of information. At an organizational level, all parties need a common understanding of how the networked entities will interoperate. All parties also need to gain consensus on procedures and trust in each other's intent to help ensure that each party has the same interpretation of distributed information and is capable of effectively acting on it.

What are the key issues to address?

A number of issues need to be overcome to turn the vision into reality. These issues include resilience, security, and the relationship between the organization and its suppliers.

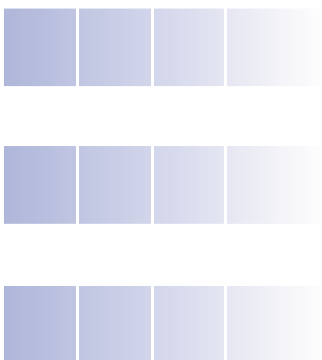
Resilient systems to support the needs of the specific military environment

Resilience is a necessity for the military enterprise. Doctrine and procedures establish a uniform way of operating by designing organizational structures and training military personnel to conduct operations. Realtime, reliable situational awareness facilitates successful planning and execution of operations. As information becomes more of a force multiplier in 21st century operations, the need for resilient information technology infrastructure is evident. However, determining how to fulfill this demand is anything but obvious.

There have been enormous advances of "off-the-shelf" information and communication technologies (ICT) in recent years. Ongoing improvements in functionality, scalability, user-friendliness and reliability render these technologies serious, affordable candidates for military operational usage. However, requirements such as mobility (including low bandwidth), autonomy, zero maintenance, and robustness place high stress on the capabilities of off-the-shelf technologies.

Security requirements call for a balanced and pragmatic approach

In military operations, the growing dependence on realtime information and its supporting technology heightens the need to safeguard both – for example, to protect against enemy attacks, insufficient system maintenance and viruses. Like scalability,



security has to be managed in a balanced way. National and international information security regulations must be met, but, ultimately, the force commander decides how to establish protection from the enemy. He must have the possibilities and capabilities to create a permanent balance among protection of information, availability of information, and maintainability of the supporting technologies – all depending on the operational situation.

A challenge for all: trusted relationships and partnerships

To support defense forces in their focused efforts toward a network-centric military enterprise, the private sector cannot stand aside. Industry has to be aware of what drives the defense forces at this point in time, including the primary intent behind their transformation process. This should help focus industry research and development (R&D) efforts for the solution needed in the next step of the transformation process.

In most cases, defense forces will have to deal with traditional requirements and acquisition processes that are based on the assumption that requirements, costs and schedules can be specified accurately. Since there is no such thing as an end state for a network-centric operation, exact specifications can not be made up front. This requires a reform of the traditional acquisition strategies and should allow for long-term partnerships or other innovative acquisition strategies.

Such partnerships also allow defense forces to get deeper insights into network-centric failures and successes in the private sector. Both parties can learn from each other, perhaps giving defense forces a better value on investments.

The first step in establishing this mutual understanding is to share information, based on a relationship of trust. Full commitment by the defense forces industry to the transformation process is needed to create an environment conducive to establishing long-term relationships between private and public entities.

The transformation process toward 21st century operations

The starting point of the transformation process is the first step toward a network-centric enterprise. It takes place in a different environment of legacy technology and thinking, depending on the national environment. Therefore, the road towards the envisioned end state, will be different by country and there will be different intermediate results in an ongoing effort for higher degrees of operational effectiveness.

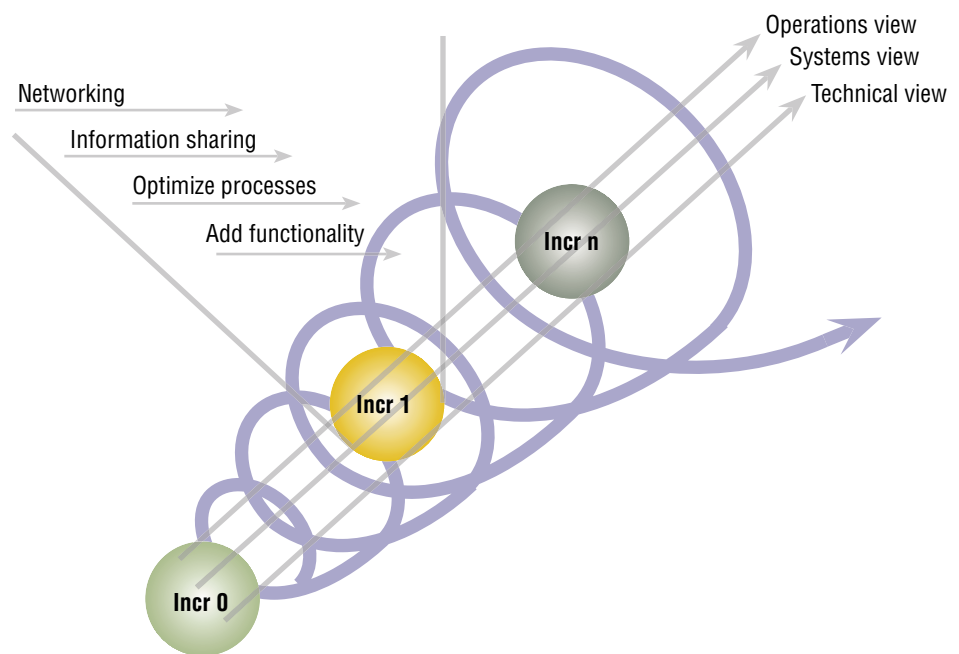
Transformation is not an end state, but a process; a process that is driven by changes in environment (threats and opportunities), fueled by innovation, and paced by institutional and cultural constraints.

Information Age
Transformation, by
David S. Alberts.

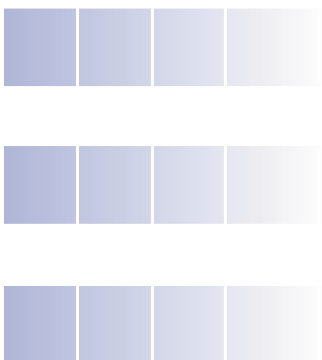
The transformation to a 21st century military enterprise starts with some basic steps. The way to achieve a higher level of network centricity has a common logic. It consists of an evolutionary process of making small steps at each stage, consisting of networking, sharing information, optimizing effectiveness, and based on lessons learned to define the functionality for the next step (see Figure 2).

Standardization supports integration when applied where necessary. In each step, agreements must be made to support transformation to network-centric operations. However, it is crucial that standardization is applied pragmatically, and that the goals of agility, adaptability and interoperability are not blocked by standardization efforts.

Figure 2. Logical components of each incremental phase.



*Note: Incr is an increment, each time progress is made, in terms of added functionality. The 0, 1 and n reinforces the idea of the progression of stages.
Source: IBM Institute for Business Value.*



Networking the force is the “entry fee”

Robustly networking the enterprise helps enable information sharing through integration of the three domains into a single network. This may sound obvious, but current practices around the globe show that this is not common. It is not common because the mobile domain has some very typical constraints, caused by limitations of bandwidth as well as by the high dynamics at the battlefield and the changing operational information needs. Dealing with these limitations requires a balanced approach toward functionality, security, mobility and costs.

To help build the foundation for a long-lasting transformation, key success factors that strengthen networking are:

- A common data exchange model offering a "common exchange language" for application interoperability
- An exchange mechanism supporting agile and adaptive information flow.

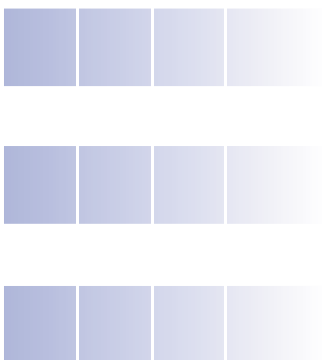
The exchange data model and mechanism offer interoperability on a logical level. An agreement on the logical level of information exchange forms the minimum basis for network-centric operations.

Achieving situational awareness by sharing information

Sharing information by use of applications leads to shared situational awareness. The first step toward shared situational awareness may seem rather modest at first glance: Initially, organizations should focus on sharing information about their own positions, the positions of other blue forces and red forces situation. This kind of information sharing in itself will have massive impact on the organization and its processes. Experience from other military transformation efforts reveals that achieving just this first step may take a number of years – not such a modest undertaking after all.

Key success factors to make progress in information sharing are:

- Convincing people to share information
- Posting information first before processing it
- Implementing measures that allow people to trust information
- Addressing issues as micro-management and information overload
- Developing procedures that support information management.



The approach to 21st century military operations focuses explicitly on these key success factors by highlighting the benefits of sharing of information as well as the enrichment of information that can follow. Information management is a critical part of the entire transformation process. It relies on managers who handle the timeliness, reliability and accuracy of information. Knowledge managers must document lessons learned and know where to find critical knowledge in unforeseen circumstances. In short, effective information sharing helps enable commanders to make decisions based on relevant and reliable information.

Develop new processes that are increasing effectiveness

With the ability to share information more easily and effectively, it is possible to redefine operational processes. One of the new processes possible is self-synchronization – aligning behavior and processes based on a shared operational picture. Another process is parallel planning. Parallel planning is based on the capability to share information realtime throughout the network. The planning process then can be executed in parallel on more places in the network instead of in the traditional sequential and hierarchical way, thus achieving faster and more reliable planning products.

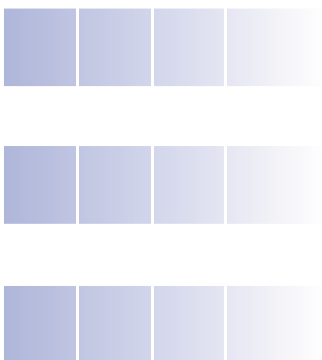
Processes like self-synchronization and parallel planning rely on a "command intent"-based approach to Command & Control, where soldiers are trained to understand command intent and act on it. At this stage of the approach, elements like leadership and personal skills are crucial to make organization-wide process changes possible.

Keep adding functionality based on experiences and lessons learned

After a cycle of efforts to improve networking, information sharing and increasing effectiveness of the processes, the requirements can be formulated for new functionality to be added in the next phases. More useful enhancements are likely when the requirements are based on actual end-user experiences and demands.

Match between operations – systems and technical view

Network-centric operations affect the entire organization and must be deeply rooted and well integrated, especially when it comes to designing how operations in all domains are linked. This requires an overall architectural framework because it is not possible to simply apply new technologies to existing infrastructures, systems and organizations or business processes. The architectural framework for network-centric operations gives a comprehensive, integrated view of the network-



centric military enterprise, including the administrative and operational processes, organizational structure, underlying information and communication systems, and technical infrastructure.

Supporting role of the defense industry

So far, a transformation process has been described that structures the key elements required to achieve network centricity and its associated benefits. This section looks at some of the supporting processes that have proved beneficial in making significant progress in network-centric initiatives around the world.

Sharing lessons learned from the commercial sector

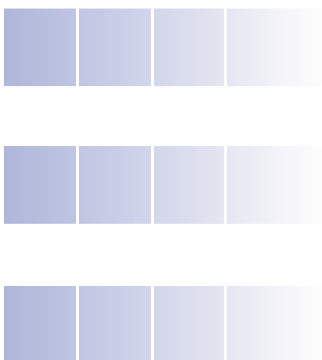
Profound changes face armed forces that are going through transformation to a network-centric enterprise. Though the concept may be relatively new to military leaders, many commercial organizations have achieved a similar transformation. For example, military organizations have begun assessing what is core to the military domain. Continued focus should be on maintaining direct control of those competencies that can make a difference in mission completion and selecting strategic long-term partners that can manage the non-differentiating activities at a lower cost with a higher level of quality. Such networked and "componentized" organizations are reconfigurable based on specific requirements, offering a competitive advantage on the battlefield.

Of course, military-specific elements need to be addressed, but past and present experiences from the commercial sector can serve as a model for military transformation toward network centricity. Commercial sector efforts demonstrate that an integrated approach is required to address everything from overall change management to modification of the organizational infrastructure or governance structures. One of the most prominent results of commercial sector transformation is a larger span of control and flattened hierarchy, which, in turn, demands new skills and capabilities from the affected people and organizations.

Reliable partners

Traditionally, defense organizations have purchased military capability in the form of platform-based projects without having to recognize the importance of integrating those systems with each other and with the systems of other organizations. A network-centric approach means that:

- The need to interface and communicate with the broader enterprise will be as important as the requirements relating to military capability.
- Partners will be required who understand how to design and implement the doctrine and people-based change program that will enable the organization to make effective use of the technology it has implemented.



Recent experiences in Afghanistan have shown that we have certainly not lost our ability to innovate under fire. We must all work hard to make this spirit of innovation not a wartime-only event, but part and parcel of everyday life.
Information Age Transformation,
by David S. Alberts.

Ultimately, implementation of the transformation is the military organization's responsibility. But partners should be committed to the transformation objectives, necessitating trusted relationships and mutual understanding. These public/private partnerships are based on long-term relationships that surpass the traditional customer/supplier relationship because defense partners are actually sharing some risks and benefits. Establishing a "smart buyer" organization offers the possibility to contract with partners innovatively, including private finance initiatives, where certain phases are financed by the partner.

Driving innovation

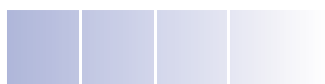
In the transformation to become a network-centric military enterprise, the role of research and experimentation is essential. For a military organization, several fundamental issues require specific solutions.

First, the input from research organizations will drive innovations, which are needed to reinvent the military organization continuously to stay ahead of "competition." The ongoing budget pressures facing defense forces today are straining the internal research capability. As a result, defense forces should leverage their research investments with trusted defense industry partners.

The second reason for driving the relationship with other research units is the need for experimentation. Over time, progress toward a network-centric military enterprise will be made through controlled experimentation in environments where experimentation is encouraged. The outcomes of these experiments (not necessarily being tested in labs, but in real practice) should flow back into product development. The loop among testing, fielding and rolling out solutions should be as short as possible.

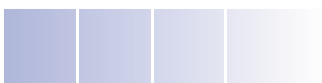
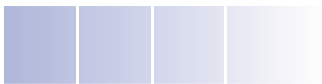
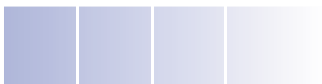
From the results of the phases in the evolutionary process follow components and systems that have to be procured. Procurement should be supportive of the overall transformation process and should have the flexibility needed to deal with an incremental, evolutionary development of the network-centric operations architecture.

Finally, it is important to team with research organizations that also have in-depth knowledge and experience with commercial sector solutions, since much of the innovation in the military domain can be derived from solutions from the commercial sector.



Conclusion

Adopting the notion of network-centric operations is revolutionary, while the transformation to a network-centric military enterprise is evolutionary. This transformation involves the entire organization, from beginning to end, from the culture to the technology, from strategy to operations. Starting to undertake incremental steps along this path requires very close relationships with organizations that understand the impact and magnitude of this transformation through first-hand experience.



Contacts

Contact for network-centric operations

Leendert Van Bochoven is the network-centric contact on the IBM Network-Centric Solutions team. Leendert can be contacted at L_van_bochoven@nl.ibm.com.

Defense contacts

John S. Fairfield, Lt Gen, USAF (Retired), Partner, IBM Defense Industry/Global Defense Industry Leader. John can be contacted at john.fairfield@us.ibm.com.

Susanna Mason, IBM Business Consulting Services, European Defense Industry Leader. Susanna can be contacted at susanna.mason@uk.ibm.com.

Stewart Lamond, IBM Business Consulting Services, Australia Defense Industry Leader. Stewart can be contacted at stewart.lamond@au1.ibm.com.

Krishna Giri, IBM Business Consulting Services, Singapore Defense Industry Leader. Krishna can be contacted at krishnag@sg.ibm.com.

Contributors

Marc Le Noir, IBM Institute for Business Value, European Public Sector Lead. Marc develops fact-based strategic insights for senior business executives around critical industry-specific and cross-industry issues. Send an e-mail to bva@us.ibm.com for more information or contact Marc at marc.le.noir@be.ibm.com.

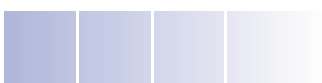
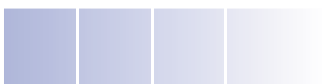
Leendert Van Bochoven, Dutch Defense Industry Leader, Partner, IBM Business Consulting Services, The Netherlands. Leendert can be contacted at L_van_bochoven@nl.ibm.com.

Scott Padgett, Business Unit Executive, World Wide Government Industry Software Sales, IBM United States. Scott can be contacted at smpadgett@us.ibm.com.

David S. Waxman, Consulting Architect, Public Sector/Homeland Security, IBM Software Group, United States. David can be contacted at dwaxman@us.ibm.com.

Randy Moulic, Research Staff Member, IBM United States. Randy can be contacted at rmoulic@us.ibm.com.

Jason Franklin, U.K. NEC Program Co-ordinator, IBM Business Consulting Services, United Kingdom. Jason can be contacted at jason.m.franklin@uk.ibm.com.



Emil Sjörup, Business Development Executive, Defense Client Manager, Principal and Lt Colonel (Retired), IBM Sweden. Emil can be contacted at emil.sjorup@se.ibm.com.

Martin Nitsche, Senior Consultant, Go-to-market Team for Defense in Germany, IBM Business Consulting Services, Germany. Martin can be contacted at martin_nitsche@de.ibm.com.

Stephen M. Bahr, Managing Consultant, Defense U.S., Colonel, U.S. Army (Retired), IBM Business Consulting Services. Stephen can be contacted at stephen.bahr@us.ibm.com.

Michael Gannon, Defense Industry, IBM Business Consulting Services, Canada. Michael can be contacted at mgannon@ca.ibm.com.

Special acknowledgement to

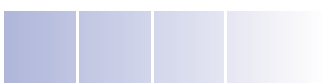
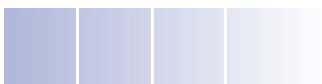
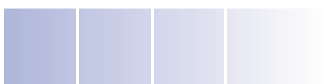
LtKol (Retired) Jacques Emmen, Managing Partner of Reinforce B.V, jac@reinforce.nl.

LtKol (Retired) Lex Bubbers, Managing Partner of Reinforce B.V, lex@reinforce.nl.

Reinforce can be reached at www.reinforce.nl.

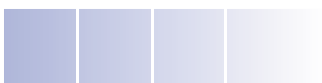
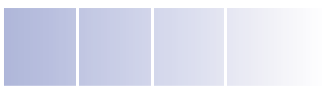
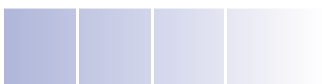
About IBM Business Consulting Services

With consultants and professional staff in more than 160 countries globally, IBM Business Consulting Services is the world's largest consulting services organization. IBM Business Consulting Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value.



References

- ¹ The term network centric operations is used to cover the transformation process toward 21st century ways of operating in the full spectrum of operations. The commonly used term network centric warfare might indicate a focus on warfare. Network centric operations is more broadly applicable.
- ² Network Centric Warfare, Department of Defense, Report to Congress, 27 July 2001.
- ³ Alberts, David S., Garstka, John J., and Stein. Network Centric Warfare 2nd Edition. www.dodccrp.org
- ⁴ Ibid.
- ⁵ Ministry of Defense, "Operation TELIC – United Kingdom Military Operations in Iraq", Report by the comptroller and auditor-general, HC 60 Session 2003-2004. 11 December 2003.
- ⁶ Ibid.
- ⁷ Edward A. Smith, Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War. A Command and Control Research Program (CCRP) publication, November 2002.



Bibliography

Alberts, David S. and Richard E. Hayes. *Code of Best Practice for Experimentation* (CCRP Publication Series). CCRP Publications Distribution Center, 2002.

Alberts, David S. *Information Age Transformation: Getting to a 21st Century Military*. CCRP Publications Distribution Center, 2003.

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age*. CCRP Publications Distribution Center, 2003.

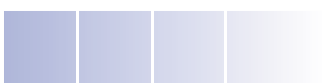
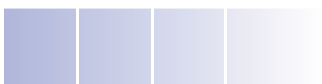
Alberts, Davis S., and others. *Understanding Information Age Warfare*. CCRP Publications Distribution Center, 2001.

Moffat, James and David John Howard. *Complexity Theory and Network Centric Warfare* (Information Age Transformation Series). CCRP Publications Distribution Center, 2003.

Potts, David and Dennis Chute. *The Big Issue: Command and Combat in the Information Age*. CCRP Publications Distribution Center, 2003.

Renner, Scott. *Building Information Systems for Network-Centric Warfare*. Presented at C2 Research and Technology Symposium, Washington, D.C. June, 2003.

Smith, Edward Allen. *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. CCRP Publications Distribution Center, 2002.





© Copyright IBM Corporation 2004

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
04-04
All Rights Reserved

IBM and the IBM logo are registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.