Navigating toward net-centricity

Insights from defense organizations leading the race for information superiority
IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive brief is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business 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.
Navigating toward net-centricity
Insights from defense organizations leading the race for information superiority
By William R. Phillips, Frans Picavet and John Reiners

The defense industry is undergoing a transformation from the industrial to the net-centric age. The goal of network-centric operations is now widely accepted, yet getting there is proving difficult. Given the scale of the challenge, are defense leaders confident about making the changes required to break through their industrial-era patterns – and complete their progression into the net-centric age?

Navigating toward net-centricity
Insights from defense organizations leading the race for information superiority
By William R. Phillips, Frans Picavet and John Reiners

Executive summary
The volume of information available to support military operations has grown dramatically, and this information needs to be shared across a wider network of coalition partners, suppliers and external agencies. Meanwhile, the nature of warfare is changing, as sophisticated new technologies are becoming readily available to a wider range of enemies. Additionally, the threat of cyberwarfare is increasing attention on information security. Faced with these challenges and threats, defense forces have little choice; they will need to further enhance both their offensive capabilities and their defense against information-based attacks.

Much has been written about the opportunities presented by the concept of network-centric operations (NCO) and the challenges that need to be overcome. These messages are now widely understood by defense forces.

The more urgent question is how to undertake the journey, actually delivering improved effects and tangible benefits. This paper shares the key lessons that military organizations are learning en route to the effective application of NCO. The focus is on those things that military leaders have direct and immediate control of, not those things that they must rely on others (namely civilian leaders) to accomplish.

Our experience and the lessons learned by our clients have revealed six critical success factors that must be addressed if the full operational concept of NCO is to be achieved. The importance of these factors is supported by an international survey conducted by IBM in September 2007 that explores defense forces’ progress in implementing NCO.
These factors are:

1. **Agreeing on the NCO destination:** Understanding the extent of transformation required throughout the organization and the need for a range of enabling projects in related areas.

2. **Embracing emerging technical approaches:** Basing technical development on the latest organization-wide best practices to encourage agility, flexibility and interoperability.

3. **Exploiting the latest defense-related technical solutions:** Realizing that some of the most difficult technical challenges to NCO can now be addressed with more flexible, capable and lower-cost technical solutions.

4. **Designing an effective procurement model:** Implementing procurement processes that match the particular needs of NCO, given the fast-paced nature of technological change.

5. **Addressing the change management issue:** Making the necessary changes to individuals’ skills, their roles, how they are organized and led and how they fight.

6. **Adopting a pragmatic approach to implementation:** Breaking the NCO program into projects of manageable size, targeting specific benefits and putting effective governance disciplines in place.

Today the understanding and adoption of these six factors varies. Some are widely understood and are being actively followed by some of the leading implementers of NCO; others are well understood but not quite so widely adopted. Some of the latest technical approaches and solutions are emerging from the research labs or are being pioneered by commercial organizations. We are confident that it is only a matter of time before all six become widely adopted in defense.

We conclude by suggesting immediate, practical actions that defense forces can take to develop an NCO road map. The critical success factors described here are no guarantee of achieving the goal of net-centricity. NCO as a goal is constantly shifting because the operational context, the defense ecosystem and the potential solutions offered by new technology are all rapidly evolving, often in unpredictable ways. However, the essential principles of leveraging the capabilities of the network to improve information management and interoperability remain constant.

We have titled our paper “Navigating toward net-centricity” because we recognize that progress has been made toward the goal of NCO, yet the journey ahead may appear daunting, particularly to those traveling alone. Leaders will make mistakes, and the consequences may be severe. At times, it may feel easier to turn back. However, we are confident that the journey can be successfully navigated if leaders plan carefully, use the latest techniques, learn lessons from those that have passed before and seek support from those that know the terrain ahead. There has never been a better time to undertake the journey. Ultimately its success will depend on the confidence, commitment and determination of military leaders themselves.
Navigating toward net-centricity

Lessons from network-centric operations implementations

Network-centric operations emerged as a concept approximately ten years ago. Since then, defense forces around the world have established NCO programs under a wide variety of names (network-centric warfare, network-enabled capability, network-based defense and others). But all have similar objectives: to utilize the advances offered by information technology to effectively and efficiently prosecute a new type of warfare and a wide portfolio of military missions, based on exploiting the power of the network to deliver conclusive information and decision superiority over the enemy.\(^2\)

In September 2007, IBM surveyed 55 people closely involved in the NCO programs of defense forces in 17 different countries.\(^3\) The objective was to understand the progress they have made with their NCO programs, the challenges they face across all stages of the project lifecycle (design, procure, deliver) and their plans for the future.

The results confirmed that NCO is becoming a higher priority, with 70 percent stating that NCO was more or much more important than two years ago and no one indicating it was less important. The vast majority is dissatisfied with progress to date and believes a number of significant challenges remain. However, they were increasingly optimistic that NCO will deliver operational benefits for two principal reasons. First, a number of improved technical solutions are becoming available. Increasingly, these are being proven in the defense arena.

Second, respondents have learned from their experiences to date and have greater awareness of how to design, procure and deliver their NCO programs.

For this report, we have researched the new technical solutions emerging and being deployed. We have also collated lessons learned from almost ten years of NCO projects. The aim is to identify the key things that are important to get right when undertaking an NCO project.

1. Agreeing on the NCO destination

NCO is of benefit to many areas of defense, including command and control, intelligence and logistics. Yet 44 percent of those we surveyed said that NCO is primarily about integrating multiple areas of defense, rather than improving a single area.

Before setting out on the journey, it is important to have an understanding of the destination end state, an organization-wide agreement on the NCO concept of operations. Many defense forces have been hampered in the past by defining what they mean by NCO too narrowly or by having multiple views of the NCO destination. For example, we have seen separate NCO initiatives being run independently in different areas of a defense organization, leading to expensive and complex integration problems when incompatible NCO solutions need to be joined. Similarly, some NCO projects have focused too much on implementing the technology and have failed to recognize the importance of processes, policies and supporting projects in other areas. They then
find that the latest technology will not work effectively without quality information, redesigned ways of working, flexible organization structures and trained staff.

There are typically a large number of NCO initiatives underway in different defense areas, each with different objectives. For example, some NCO projects focus on logistics, seeking to improve asset visibility and traceability throughout the supply chain thereby contributing to increased agility and operational tempo. In intelligence, NCO projects often aim to use more sophisticated analytical tools to deliver high-quality intelligence from a wide variety of sources and formats (video, voice, structured and unstructured data) to support operational decision making. And in command and control, NCO projects might be collating information from an increasing number of sensors and other data sources to support planning and execution of a broader range of mission types, often working in coalition with each other and with numerous external agencies. These projects, however, share a common purpose: to deliver improved capability to the operational commander. This can only be achieved if the NCO solutions are able to share information and work effectively as an integrated, end-to-end capability.

Defense forces increasingly recognize that although new technology is important in making NCO possible, NCO initiatives need to be much broader than IT implementation programs to be successful. Supporting projects are also needed in three other important areas:

- Providing high-quality information that is delivered at the right time to the end user
- Defining new ways of working, operational processes and changes to doctrine
- Changing people’s skills, roles, organizational structures and even potentially the “corporate culture” of the defense force.

Figure 1 provides an example of the typical range of issues and challenges that NCO projects will need to address, in this case in the intelligence area.

![Figure 1](image-url)

**Figure 1. Range of issues facing defense intelligence.**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Information</th>
<th>Process</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Stove-piped architectures, networks and applications, which result in a fragmented view of the intelligence picture</td>
<td>• Balancing between “need to know” versus “duty to share” and providing commanders with tools to use a risk-based approach to managing the balance</td>
<td>• Processes determined by legacy IT architecture; need greater agility</td>
<td>• Centralized, hierarchical structures are inconsistent with information sharing and collaborative intelligence production</td>
</tr>
<tr>
<td></td>
<td>• Unable to exploit intelligence across domains and across intelligence “stovepipes”</td>
<td>• Determining provenance, auditability and traceability of information</td>
<td>• Insufficient skills in key areas; need newly defined roles for data analysts and intelligence analysts</td>
</tr>
<tr>
<td></td>
<td>• Slow adoption of most advanced intelligence tools for information exploitation</td>
<td>• Need for an information management architecture</td>
<td>• Culture and frequent rotation discourages growth of key competencies</td>
</tr>
</tbody>
</table>

Source: IBM Institute for Business Value.
Many commercial organizations face similar situations. With globalization and competition intensifying, they are looking to exploit information technology to provide increased agility to respond more quickly to market and regulatory changes and to change their business models. Many organizations see information as an underexploited competitive asset. They are seeking to move away from stove-piped sources of information (by department, business unit or geography) to an enterprise-wide view, providing a common picture of operations to support decision making. Commercial organizations, too, are opening their systems and increasingly sharing information with a wider ecosystem of customers, partners, subcontractors and suppliers.

This complex, multidimensional nature of NCO is not new; it has been described before. And our survey demonstrates that many defense forces have an increasingly sophisticated understanding of the nature of NCO programs; they recognize that NCO requires an integrated approach and attention at all stages of the defense “value chain.” However, the most important point is that this understanding must be translated into how they define the NCO destination and the journey.

Organizations need a shared view of how they will operate in the net-centric future. This should include a high-level systems architecture, but also an information architecture and an understanding of the implications for military doctrine, working-level processes, skills, roles and organizational structures. This view needs to be shared across all lines of development and departments of the organization, so it is clear how network-enabled support functions can help the operational commander.

2. Embracing emerging technical approaches

Forty-six percent of respondents cite the availability of new technologies as the main impetus for pressing ahead with NCO.

Many defense forces have bought into the NCO concepts of an integrated systems architecture and interoperability, but have had considerable difficulties making them happen because of the complexity of their existing systems. Most defense forces have a vast number of legacy systems that are often bespoke and based on proprietary standards from many separate vendors. These systems are often inflexible and expensive to maintain, with changes to one system having a domino effect on other systems in the network. It is difficult for these systems to communicate, and this problem is multiplied when trying to share information with coalition partners. Despite the fact that commercial software suppliers offer better, more reliable, lower cost and more flexible solutions, we still see defense forces seeking custom-built information systems.

New technical approaches, now being widely implemented in commercial organizations to address similar problems, offer a potential solution. Service-oriented architecture (SOA), information management and an open approach to systems development are not technologies as such; they are more like technical philosophies, which together aim to deliver information to end users across the organization in more flexible ways, by aligning the information technology to business and operational needs (see Figure 2).
These three technical approaches are mutually supportive in providing NCO solutions. A service-oriented architecture depends on enterprise-wide information and an open approach, which increases flexibility and interoperability. Together, they potentially provide higher-quality information, delivered in more effective ways to support decision making, greater agility and interoperability. Because organizations are not locked into proprietary systems, application development and maintenance costs should also be lower.

Commercial organizations across many sectors are rapidly embracing these new technical approaches. For example, in oil exploration, SOA is seen as a way to reduce dependence on expensive legacy IT systems and to provide the flexibility and interoperability required when setting up new applications in remote areas, with a new supply chain, new subcontractors and new suppliers. From the information management standpoint, global consumer goods companies are developing strategies to manage their information...
Navigating toward net-centricity worldwide. They are seeking to standardize information and supporting systems and processes so that they can deliver high-quality information, a single source of the truth. This will provide them with the consistent, reliable information needed to make management decisions at a global level and serve their customer base. Custom-built software applications are rare in the commercial world, as users increasingly demand the standard commercial off-the-shelf (COTS) products of mainstream software suppliers.

Defense organizations are increasingly recognizing the potential of these technical approaches. International bodies, such as NATO, the NCO Industry Consortium (NCOIC) and the International Technical Alliance (ITA), are carrying out productive research into the application of these approaches to defense. The NCOIC is an organization of approximately 100 members – private sector companies, academic institutions, non-government and government agencies – that are collectively addressing the challenges of standards and methods to enable the concepts of NCO. The ITA is a partnership between the UK Ministry of Defense and the US Army, led by IBM to explore the basic science underpinning the “network” and share technical progress and solutions.

Defense organizations are also actively communicating the benefits of adopting these approaches. When we asked our survey respondents to rank the new technologies that were important in delivering NCO, SOA and information management were among the highest (see Figure 3), when they probably would not have featured at all a few years ago.

Defense forces are also making progress in deciding how to take these approaches forward. For example, in the United Kingdom at the 2007 Coalition Warfare Interoperability Demonstrator, a federated approach to the implementation of SOA was trialed. Scenarios were used to highlight how more effective command and control could be provided across coalitions by facilitating the quick and cost effective flow of information and rapid creation of a joint operational picture. It also provided insight into how defense forces can incrementally and cost effectively develop new capabilities by building on rather than replacing existing legacy systems.

**FIGURE 3. Which technical innovations are most important for NCO?**

![Chart showing percentage of respondents ranking different technical innovations as most important for NCO.]

*Source: IBM Services Products and Defense Exchange conference survey, 2007.*

New technical approaches, such as service-oriented architectures, information management, and open standards and architectures, can help defense organizations improve information quality, agility and interoperability.
There is little doubt that, in the future, more and more NCO projects will have these new techniques as a key component. However, designing, procuring and implementing such organization-wide approaches will present a new set of challenges.

3. Exploiting the latest defense-related technical solutions

A number of other technical innovations were identified by respondents as being important, including security, decision support and realtime systems.

We can only go so far in recommending that technical innovations pioneered in commercial organizations be emulated in the defense arena because of four particular challenges dictated by the nature of defense operations:

- Maintaining the security of sensitive information
- Providing high availability of systems in a range of difficult situations
- Providing information in realtime to facilitate accurate and rapid decision making and closer synchronization between sensors and effectors
- Providing systems with the mobility required for modern military operations.

Technical solutions, however, are available that address these concerns, as recognized by our sample’s responses shown in Figure 3. In the past, these solutions were often bespoke, with high maintenance costs and limited flexibility and interoperability. However, more and more solutions, which use standard software components compatible with the organization-wide technical approaches discussed earlier, are now becoming available. Research work is ongoing among commercial software suppliers and collaborative research bodies, such as the ITA, with the promise of yet more capable solutions available soon.

Security concerns have been a significant challenge to the concept of NCO from the start. With multilevel security structures (e.g., Confidential, Secret, Top Secret), most IT systems have been designed with physical separation between the levels (i.e., an “air gap”) – making networking practically impossible. It is becoming increasingly difficult to defend systems from determined efforts to gain access, as demonstrated by the growth in volume and sophistication of “cybercrime.” Cyberwarfare has recently become a major concern. For example, Estonia’s state systems were targeted in May 2007 in a concerted denial of service attack. Resolving the security challenge is more than just a technological problem. Security policies and procedures are normally controlled by national bodies outside defense organizations. Plus, in a coalition, security classifications and policies of the partners can differ dramatically. Changing security policies does not happen easily and requires significant political will.

Security solutions are emerging that provide some hope that these challenges can be overcome. For example, more sophisticated approaches to labeling and managing data flows and the use of guards are proving successful in managing data flow in multilevel security structures. Methods for validating access rights are becoming more sophisticated (e.g., VPN security combined with the use of biometrics and location data). Research is at an advanced stage in developing more cost-effective approaches to security through an SOA-based approach. There is still some
way to go, but developing and implementing more-secure technical solutions is an essential prerequisite to gaining the level of international agreement required for NCO.

A similar picture emerges when looking at the other challenges. More reliable and sophisticated software (e.g., software monitoring, building in system redundancy) is helping increase systems availability. The growing requirement for realtime solutions in the commercial sector (e.g., to support financial trading) means that defense organizations have access to more realtime solutions based on commercial software and standard components. Realtime solutions are consequently available at a lower cost and are easier to integrate with other systems. Mobile solutions, often based on an SOA approach, are increasingly capable and portable, making use of increasingly sophisticated applications (e.g., situational applications).

Defense forces have started deploying many of these solutions with success. For example, the US Army’s Maintainer’s Remote Logistics Network (MRLN) program used commercial software installed in vehicles linked via bidirectional data radios to central maintenance and logistics systems. The aim was to improve the responsiveness of its maintenance resources and platform availability. The Finnish Defense Forces, as part of their Network-Enabled Defense initiative (FiNED), have set up a Center of Excellence with IBM to test SOA-based solutions for the defense environment. They have successfully completed three proof-of-concepts so far, including:

- Scaling SOA applications down to the laptop level with the ability to continue to function in disconnected mode and to rapidly establish the common operational picture once reconnected
- Mapping to NATO’s definitions of core enterprise services and standards
- Proving legacy systems, proprietary systems and other government systems can interconnect during crisis situations.

4. Designing an effective procurement model

Sixty percent of those surveyed described their procurement processes as ineffective, given the particular requirements of NCO.

Today’s procurement processes are too slow, relying on processes and procedures that were created in the industrial age and do not meet the military’s needs for NCO. A lengthy procurement process often means that solutions and technology are outdated the moment they arrive. Defense organizations need a new procurement model that includes:

- A more agile approach that recognizes the spiral nature of NCO development and the fact that long drawn-out approaches to platform-based procurement are no longer suitable
- A higher degree of coordination across departments, moving away from current stove-piped procurement
- Sponsorship and commitment, as the initial benefits of NCO are often difficult to measure and support needs to be sustained
- Improved commercial relations with suppliers to increase supplier performance and sharing of risk.

More agile procurement for NCO is possible through a combination of quicker processes and greater flexibility. Tempo can be increased by breaking down programs into reasonable sizes and avoiding over-ambitious design and unnecessarily detailed requirements gathering.
By identifying a smaller number of strategic suppliers and setting up framework-style agreements, the number of lengthy procurement exercises can be reduced. To gain flexibility, leaders must understand the spiral nature of NCO, refrain from producing overly detailed requirements and promote the use of commercial off-the-shelf applications and open standards and architectures.

A coordinated approach to NCO procurement can be difficult given the large number of different projects that may be underway and planned. Procurement will take place at multiple places in the organization. In these circumstances, a “light portfolio” approach to procurement is likely to be more successful than a centrally imposed directive. In a portfolio approach, a central authority would be responsible for mandating standards and overall technical approaches, while giving other levels freedom to procure within these parameters. The central authority would review new purchases to help ensure general compliance rather than impose a “system of systems” approach to NCO.

Strengthening commitment depends on communicating a convincing business case to a wide range of decision makers and influencers. The NCO program needs to be seen as being business- and outcome-driven (rather than as an internal procurement process or an IT program). Tangible benefits need to be identified. Ideally these should be in high-priority and high-visibility areas. It is important to look for specific opportunities for quick wins, which can be used to maintain the enthusiasm for the project.

Commercial relations need to become more productive, recognizing the long-term and strategic nature of NCO programs. Strategic partnerships should be developed with a few key suppliers, with a mutual goal of establishing a long-term, productive relationship based on commitment to key principles (e.g., an SOA approach based on open standards). Most organizations will need a different procurement model to increase the productiveness of their strategic suppliers, by providing them with incentives based on outcomes and encouraging them to accept greater risk. Delivery projects should be put out for competitive bidding among a pool of capable suppliers to encourage the best value to emerge.

5. Addressing the change management issue

When asked to identify the greatest barriers to delivering NCO, respondents overwhelmingly pointed out the number of issues related to change management aspects.

It has long been recognized that delivering NCO is about more than implementing technology. Alberts, Garstka and Stein wrote in 1999 that network-centric warfare is about human and organizational behavior. They described a ceiling to the benefits that can be delivered by NCO systems solutions unless human, organizational and cognitive domains are transformed as well.

As an example, improvements in command-and-control systems have the potential to provide better intelligence, shared situational awareness and decision support to the front line. This has implications for the data analysis and IT skills required of soldiers and others.
in the command-and-control structures (as well as other skills such as leadership, decision making and working in coalitions). Command-and-control ways of working and organizational structures may need to adapt, as traditional multilayer hierarchies slow the decision making process. The networked information now available to the front line also poses some difficult questions about the organization’s culture and operating model. For example, should the organization empower those in the front line to make more decisions, independent of traditional command-and-control structures?

When we asked our survey group to identify the greatest barriers to implementing NCO (see Figure 4), many mentioned difficulties in managing change in the organization (e.g., culture change, poor sponsorship, the need to change ways of working and insufficient skills).

NCO initiatives therefore need to be broad-based and include approaches for managing the people-related aspects of change in parallel with addressing the technology and information aspects described earlier. There are a number of tried and tested approaches, as managing these issues is not new to defense or indeed to most organizations. Traditional approaches include rigorous end-to-end process design, role definition, governance and organization structure, stakeholder management, communications and change management.

However, some new techniques are now available that make it easier to integrate changes in business processes with a technology transformation. For example, Component Business Modeling (CBM) breaks down business functions into different components. Business Process Management uses metrics to monitor ongoing business performance to drive continuous improvement; and the Service-Oriented Modeling Approach aligns business component models to services-based IT reference architectures. These techniques are now being used by a number of defense forces (for example, the United States and a number of European defense forces have used CBM for different functions and at different levels to analyze defense processes and to support their transformation programs).

To fully embed NCO, defense forces must become more adept at managing organizational change.

FIGURE 4. What are the greatest barriers to achieving NCO?

Defense leaders should expect rework and realignment when managing a broad program of rapidly evolving NCO initiatives. Phased implementation, continuous measurement (albeit against frequently redefined objectives) and effective governance can improve the odds of success.

6. Adopting a pragmatic approach to implementation

Across our survey sample, 72 percent were not satisfied with progress achieved to date. When asked why projects had failed to deliver sufficient benefits, 44 percent mentioned difficulties in measuring the benefits, while 42 percent cited problems with project delivery.

NCO initiatives must compete for limited funds among many other projects and demands for resources. Because of the length of the programs and the difficulties in measuring benefits, particularly during the initial phases, it is important to maintain the commitment of the organization. NCO initiatives need to focus on delivering tangible operational benefits throughout their lifecycle. As described earlier, implementation quick wins should be targeted in visible, high-priority areas to develop an initial impetus for the project. A range of suitable metrics should be defined that can be used to measure and communicate progress in implementing NCO. Once the project has achieved traction, organizations can encourage take-up through the use of incentives. For example, it may be worthwhile to allow use of the system at a discounted cost (or even for free), as increased user participation will increase its overall value to all.

For an SOA-based transformation to NCO, we recommend a pragmatic, phased approach to implementation, as set out in Figure 5. This incremental approach is being used in Finland, where the benefits of one stage are proven before moving on to the next in order to sustain political support. An incremental approach is particularly suitable given the criticality of military IT systems; the failure of a “big bang” implementation approach could pose a threat to national security.

Because of the spiral nature of NCO development, NCO programs themselves will need to have regular reviews of progress against frequently redefined objectives. In such circumstances, it is not realistic to measure progress against tightly defined requirements. It is more important that project traction is achieved and momentum sustained, with the understanding that some degree of rework will be inevitable to fully synchronize all initiatives.
Effective discipline is needed in project governance. This is particularly important for NCO programs, as involvement and agreement are required across lines of business on key decisions such as standards, the definition of services, shared policies and procedures, and a common architecture and infrastructure. There will typically be several layers of governance, including corporate, IT, SOA and information assurance, which will need to be coordinated.

**Conclusion**

NCO programs are complex, and the target of net-centricity is constantly moving. There should be no illusions that the journey will be straightforward. However, we share the optimism of those surveyed who are working with NCO programs. Through the accumulated lessons from past implementations and the benefits of emerging technologies, positive progress can now be made in the direction of net-centricity.

Military leaders can take some immediate practical steps. First, see if there is a commonly defined view of how the organization will actually apply the concepts of NCO. Check to see if this view encompasses all areas of defense in an integrated way, as well as all the different dimensions affected (technology, information, processes and people). Assess critically the progress made to date, ideally through an independent review. Evaluate the current NCO project portfolio and compare the tools and techniques being used against the leading practices described in this paper. Identify potential strategic partners that have the breadth of capabilities, depth of experience, and trustworthiness to work toward the NCO goal. Understand the awareness of and enthusiasm for NCO and the appetite for change across the organization. After completing these initial steps, the time will be right to develop a roadmap, with specific milestones that map the route to net-centricity.
About the authors

William R. Phillips is the IBM Global Defense Leader and the Leader of the Network-Centric Operations initiative for IBM, focusing on defense and homeland security organizations globally. He is a member of the Defense Business Practices Implementation Board, which is comprised of 20 senior business executives who provide advice and council to DoD leadership as part of their business transformation initiatives. He has personally led client projects with the DoD, the US Army, the Defense Finance and Accounting Service, the US Air Force and the US Navy. He is a thought leader in the area of public sector financial management. He has been asked to testify before Congressional Committees and is the coauthor of two books about the challenges of reform and the application of entrepreneurship in the public sector. He is a frequent speaker on the subjects of financial management improvement and has published or been quoted in numerous related articles. He can be contacted at william.r.phillips@us.ibm.com.

Frans Picavet is the IBM Global Network-Centric Operations “Ambassador.” As a senior subject matter expert, he contributes to the development of IBM’s NCO policy, concepts and implementation guidelines. He has particular responsibility for working with NATO, where he previously worked as Director of the NATO Consultation, Command and Control (C3) staff and co-vice chairman of the NATO C3 Board. He has 37 years of experience with the Netherlands Army, reaching the rank of Major General. He is a frequent speaker at conferences on subjects relating to network-centric operations, in particular focusing on the technological, behavioral and organizational transformation required to achieve NCO. He can be contacted at frans.picavet@be.ibm.com.

John Reiners is a Senior Managing Consultant with eighteen years of experience directing and working on business improvement projects for both the public and private sector. He has several years’ experience on consulting projects with the UK Ministry of Defense, working on business transformation projects for Land, Sea and Air Front Line commands. He now works for the IBM Institute for Business Value, where he researches, writes and deploys studies on issues of strategic importance to the Public Sector. He can be contacted at john.reiners@uk.ibm.com.
**Key contributors**

Stephen M. Bahr, Senior Managing Consultant, Global Defense/Network-Centric Operations, IBM Global Business Services, Colonel US Army (retired)

Nigel Bairsto, European Logistics Leader, Network-Centric Operations, IBM Global Business Services, Air Vice Marshal, UK Royal Air Force (retired)

Stefan Hefter, Senior Managing Consultant, IBM Global Business Services, Defense Solutions, Germany

Grant Hume, Defense and Security Subject Matter Expert on UK C4ISR development and procurement, IBM Sales and Distribution, Lieutenant Colonel UK Army (retired)

John Palfreyman, Network-Centric Operations Solutions Leader, IBM Global Technology Services

Sami Serpola, IT Architect, IBM Global Technology Services, Finland

Mike Small, Intelligence Leader, Network-Centric Operations, IBM Global Business Services

Leendert Van Bochoven, European Leader for Defense and Network-Centric Operations, IBM Global Business Services

Cliff Wilson, Defense Industry Leader, Network-Centric Operations, IBM Software Group

**About IBM Global Business Services**

With business experts in more than 160 countries, IBM Global Business Services provides clients with deep business process and industry expertise across 17 industries, using innovation to identify, create and deliver value faster. We draw on the full breadth of IBM capabilities, standing behind our advice to help clients implement solutions designed to deliver business outcomes with far-reaching impact and sustainable results.
References


3 This survey was conducted at the IBM Services Products and Defense Exchange (SPADE) conference in Stockholm in September 2007. Respondents came from the following countries: Canada, Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Romania, Singapore, Slovenia, Spain, Sweden, Switzerland, the United Kingdom and the United States. Of those surveyed, 44 were from defense organizations and 11 were from suppliers. A number of disciplines were represented, including: IT professionals, project managers, systems end users and logistics staff. There was a mix of military and civilian personnel.


5 Some defense forces, including NATO, have already made good progress in articulating target architectures, which will help frame further discussions on how NCO will work in their organizations.

6 More information on NCOIC can be found at www.ncoic.org and about ITA at www.usukita.org.


8 “ITA: About us.” http://usukita.org/?q=about

9 IBM Global Business Services participated in this trial.


