JOURNAL OF DEFENCE SCIENCE

VOLUME 8 NUMBER 3 SEPTEMBER 2003

The Journal of Defence Science is published for the Ministry of Defence by QinetiQ Ltd. The Ministry is a major sponsor of research, evaluation and testing; its scientific and technological interests include long-term speculative research and analysis, applied research and studies to underpin equipment procurement decisions, and support to programmed procurement and in-service capabilities.

If you do not wish to receive future copies of this journal, or if your address details are incorrect, please ring +44(0)1420 525565

Ministry of Defence

Journal of Defence Science

The Journal of Defence Science publishes original papers and reviews on subjects of current relevance to the Ministry of Defence's research, development and procurement programmes. Coverage ranges from experimental reports and theoretical discussion to historical accounts and forward-looking analysis. The journal often gives prominence to a particular theme and includes expert papers at a number of levels from state-of-the-art surveys to detailed descriptions of particularly exciting lines of enquiry. The journal is normally published every four months, and over a year there is a balanced coverage of the air, land and sea environments and their military systems, and of the scientific disciplines that support them.

Defence science and technology is supported from a range of sources that includes QinetiQ Ltd, Dstl (Defence Science and Technology Laboratory), other institutes, companies and the universities. This base is likely to become broader; the journal is seen as a key element in promoting the cohesion of the defence community. Most papers are written by authors in QinetiQ or Dstl; papers from others who work under contract to the Ministry are welcome. Papers are also included reflecting collaborative research under formal international agreements. On occasion, contributions may be invited from outside experts to stimulate discussion or complement papers from normal sources.

Overall, the journal sets out to promote interest in defence science by publishing accounts that address the context of current work and supply a degree of explanation not available in other publications. The journal is intended to be readable and interesting to the militarily aware while being satisfying and stimulating to experts in other fields of defence science. Readers should thus have the opportunity to be better informed on matters outside their particular specialisms. The journal also provides a basis of reference material of continuing interest.

Advisory Editorial Board

Editorial Board

Managing Editor

Assistant Editor

The Journal of Defence Science subsumes the Journal of Naval Science, founded in 1945 as the Journal of the Royal Naval Scientific Service.

Communications to be addressed to:
The Managing Editor, Journal of Defence Science,
MoD Channel, QinetiQ Ltd, Cody Technology Park, Ively Road, Farnborough, Hants GU14 0LX

Journal of Defence Science

Volume 8 Number 3 **September 2003**

Network Enabled Capability:

Network Enabled Capability

Foreword by Capability Manager Information Superiority, Ministry of Defence

Network Enabled Capability, a phrase coined in 2002, is gaining increasing recognition in the UK Defence even though we are collectively unable yet to define its full potential. The choice of words is deliberate – a military capability that is enabled to develop its full potential through a network or networks. Within this intentionally broad conceptual and technical framework, we want to enable all those involved in developing UK Defence to be freed to do so. We want them to be constrained only by the requirements necessary to ensure that their component delivers its full potential to the whole and that it is able to maximize its own potential by drawing on the whole.

But where does this lead? The physiology of defence capability is comparatively straightforward to explain – the organizational skeleton, the senses and muscles as inputs and effects, the lifeblood of logistics flowing through the arteries, decision making in the brain, and the whole enabled by the neural network. The challenge is to develop this body in the most efficient way to meet the demands of the future. This poses two problems. First, we do not know what those demands will be and so we cannot afford to define our objective too narrowly – a potential Nobel prize-winner would suit some scenarios but might be ill suited to the Olympic Games. Secondly, we do not know of what our 'body' is truly capable when its physical and mental capacities are stretched. But I contend that both of these are not actually problems but opportunities; opportunities to evolve a balanced capability in which the harmonization of sensing, thinking and doing exceeds anything we currently imagine.

The future of Network Enabled Capability is, I believe, ours to develop. Its span is as wide as Defence itself and as deep as our imagination and our resources will allow. It must encompass all parts of the Armed Forces and embrace all scientific disciplines if it is to deliver its full value. This journal has an important part to play in stimulating the debate that will help us all to push the evolution forward.

Major General Rob Fulton

Ministry of Defence, Northumberland House, Northumberland Avenue, London WC2N 5BP

Network Enabled Capability: concepts and delivery

David Ferbrache
Ministry of Defence

Abstract
NEC harnesses network technology to facilitate radical improvements in shared awareness of force disposition and intent, together with a capability for rapid reconfiguration, and synchronization of operations. Already, the sensors, CIS and communication systems necessary for effective networking are becoming available. The challenge of NEC is to explore how systems in service or in procurement can be harnessed and integrated to increase military capability. The solution is likely to include different methods of working, streamlined planning and execution processes, questioning traditional command hierarchies, and throughout an underlying flexibility to reconfigure and restructure in response to operational circumstances. At all levels, getting value from NEC requires readiness to examine novel concepts of use, specification, development and procurement. Though not without significant challenges, the effective introduction of NEC is unlikely to be baulked by insurmountable technical hurdles; the greater need will be for a shift in thought processes and methods of working, so that issues are instinctively thought of in NEC terms.

WHAT IS NEC?

Network Enabled Capability was born out of the Strategic Defence Review: New Chapter and signalled a commitment by the Ministry of Defence to exploit the potential of improvements in network technology to facilitate radical changes in the way we structure and deliver defence capability. Since that announcement, MoD has worked to turn rhetoric into reality by seeking to explore the concepts underpinning NEC by seeking opportunities to integrate and achieve greater gearing from our investments in future sensors, weapons and platform systems, and by introducing the capability that engineering principles and processes require to scope, specify and acquire integrated future systems.

In the words of SDR New Chapter, NEC is founded on the principle that achievement of a networked force allows:

- shared awareness
- agility
- synchronization.

Awareness includes the sharing not only of information on the immediate environment and intentions of our own, enemy and neutral forces, but also the development of shared command intent and understanding.

Agility captures our ability to reconfigure forces and structures rapidly, building on this shared awareness, exploiting effective mission planning methods, and enabled by an information environment that allows rapid reconfiguration of the underlying network and knowledge bases.

Synchronization captures our ability to plan for and execute a campaign in which we can ensure all elements of the force work together to maximum military effect by synchronizing the execution of their missions to mass forces or generate coordinated effects on target.

SO WHAT?

The concepts of awareness, agility and synchronization offer opportunities for conducting military operations in very different ways, or for optimizing the execution of current military doctrine. The challenge is to explore the potential offered by NEC in concert with military concept developers in an environment where the options can be explored and the benefits harnessed.

The US Office of Force Transformation has set out a vision of how future warfare may be conducted based on the objective of self-synchronizing forces that can work together to adapt to a changing environment, and to develop a shared view of how best to employ force and effect to defeat the enemy. This vision removes traditional command hierarchies and empowers individual units to interpret the broad command intent and evolve a flexible execution strategy with their peers. This vision is challenging and may indeed represent the nirvana of US network centric warfare, but there are many steps along the journey.

The UK Joint Doctrine and Concepts Centre (JDCC) is producing a high-level operational concept that seeks to provide a credible response to the changing security environment, and includes:

- a joint operational picture (JOP)
- collaborative planning
- mission-organized force elements
- effects-based operations
- enhanced tempo.

The JOP is a fused and integrated situational awareness knowledge base that allows all force elements to access and contribute to a common understanding of the operational environment. The benefits of the JOP include improved combat identification, an ability to build and maintain a deep and broad view of the battlespace, and greater confidence in the consistency and accuracy of the picture, including improved sensor fusion.

Collaborative planning includes an ability to streamline mission planning, drawing in skills and expertise from a wider range of organizations and staff, as well as allowing parallelism in the development of detailed plans, critical reviews of planning assumptions, and a shared understanding of intent and objectives.

Mission-organized force elements refer to our ability to design force packages for specific scenarios, and to be able to reconfigure and restructure our forces in response to changing operational circumstances, rather than assuming fixed and inflexible structures based on peacetime configurations or pre-prepared plans.

Effects-based operations includes an ability to move from thinking in terms of forces employed against the enemy, to a deeper understanding of what we are really trying to achieve in terms of influence, coercion, deterrence, attrition or destruction. It includes an ability to use (and model the likely impact of) a far more flexible set of effectors –not just 'kinetic' weapon systems but psychological operations, deception, electronic warfare, computer and network attack –all set in a context that is coordinated with broader government activities and operations.

Enhanced tempo refers to the streamlining of planning and execution processes to allow rapid application of effects in a manner that responds quickly to the changing circumstances of the military operation. Fastest is not always best –but the key is to be able to plan and react within the decision-making cycle of the adversary.

These elements set the scene for a different way of conducting future warfare but one that will be dependent on the network delivering, and in the confidence our military colleagues have in the ability of the network to underpin these concepts.

JUST DIGITIZATION BY ANOTHER NAME?

MoD has had many initiatives that have sought to digitize elements of our forces and capabilities. .Digitization of the Battlespace, Joint Command Systems Initiative, Joint Battlespace Digitization. While NEC is born of this stable, it has a different focus and objective. We are now delivering the network –BOWMAN, FALCON, Skynet V, JTIDS, CEC, JCSI, as well as delivering the sensors –PICASSO, SOOTHSAYER, ASTOR, WATCHKEEPER, RAPTOR. The key challenge is now to harness these systems and to understand the opportunities to integrate and optimize military capability, while continuing to invest in the future enablers. NEC only has value in an operational context; it does not value the network for its own sake but only as an enabler for the delivery of real military effect. As such, the key challenge for NEC is engaging the military operators to explore and understand its potential, to refine concepts and doctrine, and to build capability across all lines of development.

WHY THE FOCUS ON EXPERIMENTATION?

To assist in this process, we need to engage our military colleagues in an environment that allows them to understand the opportunities offered by NEC, to refine their concepts of employment for future systems, and to work with the acquisition community to build real capability. Experimentation is at the heart of this approach, exploiting both synthetic environments and live trials/exercises as the vehicles for exploring and demonstrating alternative concepts of employment for future systems, and also the benefit of improved integration and interoperability between elements of the system of systems.

The creation of an NEC experimentation environment requires an ability to build a federation of synthetic (and potentially live) system elements, a credible set of baseline architectural assumptions and, most critically, the support of the military in providing the expertise required to engage in experimentation. We are entering into a unique partnership with industry through the NITEworks initiative to deliver not only the experimentation environment but also the access to the industry expertise and skills needed to identify and realize the benefits of NEC. NITEworks provides a hub for the NEC experimentation federation, a partnering and intellectual property structure that allows wide industry engagement, and a catalyst for business change in MoD to embrace experimentation as an integral part of capability development processes. NITEworks and the Command and Battlespace Management ARTD at Dstl Portsdown West provide the basis for effective links with the US Joint Forces Command and NATO Allied Command Transformation experimentation facilities and multinational experiments. This is regarded as key to influencing US transformation thinking to consider the future impact on coalition operations.

The linkage to collective training systems such as the Combined Arms Tactical Trainer is vital, enabling us to augment existing training environments to introduce simulations of future capabilities, to piggyback on established training and exercise activities. In a similar vein, the development of a synthetic augment to the range instrumentation at the British Army Training Unit Suffield also allows us to introduce new systems such as ASTOR and UAVs into exercise play, as well as providing flexibility and depth to brigade-level training. While exercises offer potential for experimentation play, there will always be a tension between training of the force and wider-ranging exploration of new capabilities that may not enter service in the near term. MoD will need to accept that NEC requires a commitment to experimentation, which carries with it force structure implications in terms of providing for appropriate experimentation forces in an already heavily committed defence force.

IS THIS A SYSTEMS PROBLEM?

NEC is a systems and capability engineering problem, and many of the measures we need to deliver NEC will address weaknesses in our broader capability engineering processes. Since the formation of the Equipment Capability Customer (ECC), MoD has sought to develop equipment capability rather than focus on individual platforms and systems. Processes have been instituted for annual capability audit, still subjective in the main, but a discipline that was lacking in the previous organization. Directors of Equipment Capability (DECs) are encouraged to think in capability terms, and to lead on cross-cutting reviews of capability areas such as Joint Situational Awareness, Joint Secure Information Exchange and Joint Collective Training. A major pilot study has also been underway, Kill Chain Development (KCD), aimed at an end-to-end review of the effectiveness of our time-sensitive targeting capability. KCD required the ECC to look across the whole surveillance, targeting, weaponeering, platform tasking, weapon release, effects on target and battle damage assessment cycle. This review allows the ECC and our customers (the military front line) to identify opportunities for improved integration of systems, refinement of equipment capability, and also changes in tactics, techniques and procedures.

While these initiatives move us towards an effective capability engineering structure, we still have a long way to go. The ECC needs to develop a high-level view of capability requirements rather than focusing on user requirement documents, which can be project specific and occasionally drift into the solution space. We also need to develop the tools and environment to enable DECs to relate their requirements to those of other DECs – and to understand how the system as a whole functions and can be optimized. This development also needs to consider the interplay between platforms/effectors and the enablers – sensors, information and communications infrastructure – that support them. Realizing this objective will require a more effective operational analysis framework which ensures that the balance between enablers and teeth capability is addressed, and an integrated approach to concept development. The end objective is to establish a capability engineering environment that sets the work of each DEC in context, provides the basis for incentivizing cross-DEC working, and enables the Joint Capabilities Board to focus on pan-capability issues.

This capability engineering environment must extend across the acquisition community as a whole, allowing the Defence Procurement Agency and Defence Logistics Organization to respond to user requirements that are contextualized, can be linked to an integration process that considers the systems architecture, allows integrated project teams to work together to identify opportunities for optimizing systems of systems, and also ensures consistency of assumptions regarding enablers and project interdependencies.

Work is underway to ensure that our approvals processes require projects to illustrate their dependencies on other projects at the point of approval, using architectural viewpoints derived from the DOD architectural framework. The ECC will also be reviewing its test and evaluation policy and associated infrastructure with the aim of developing an acceptance regime in which projects are accepted against higher-level user requirements rather than system performance requirements. This requires an ability to mix synthetic and live evaluation, and to be able to demonstrate end-to-end operation of projects as part of the broader system.

In short, delivery of NEC requires us to address many broader capability-engineering issues and processes in MoD, and in doing so realize many of the aims of Smart Acquisition as originally postulated during the Strategic Defence Review.

ANY TECHNOLOGY CHALLENGES?

NEC is not a technology-centric initiative, it is about harnessing the potential of technology in an operational context, and about developing the processes and culture that can deliver NEC.

Nevertheless, there are technology challenges hidden within NEC, challenges about the interaction of people and technology. Key to NEC is an ability to move beyond communications and information infrastructure to a scientific basis for structuring the information environment in which our forces operate to provide effective situational awareness, support collaborative mission planning and allow force synchronization.

This requires a better understanding of human cognition and perception, as well as a deep understanding of the range and diversity of approaches to command decision-making and the communication of intent.

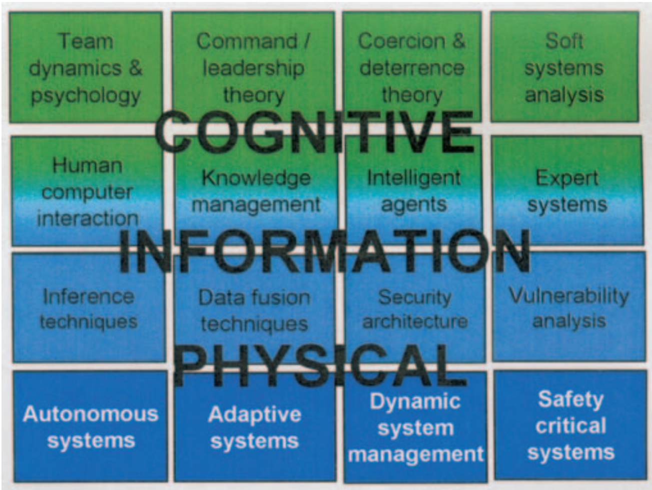


Fig 1. Technology enablers for NEC

The achievement of NEC will also require continued development of information management techniques ranging from low-level data fusion and signal processing techniques, through inference and expert systems, to intelligent agent technologies and the means to engineer effective human / computer interfaces capable of providing the rich environment that promotes effective user interaction.

Self-synchronizing forces' structures and greater use of autonomous system elements will raise challenges of adaptive system design, dynamic systems management and safety critical systems.

Lastly, NEC is not without risk, and in particular a risk of dependency on technology, and an inability to revert to previous processes and force structures. This may raise issues of vulnerability to asymmetric attack, and may also limit our ability to interoperate (and certainly integrate) with less sophisticated coalition military forces.

WHAT NEXT?

NEC remains the highest priority for the Equipment Capability Customer. Its achievement raises issues of communicating and engaging with the front-line military; of reviewing and challenging our current military concepts; of developing the systems and capability-engineering processes required to deliver NEC; and finally of ensuring continued investment into the key underpinning technology areas.

NEC is a journey not a destination; we have many more steps to take along this journey and much that we need to share with our allies as we move forward together.

Ministry of Defence, Northumberland House, Northumberland Avenue, London WC2N 5BP
ferbrache@btinternet.com

Network Enabled Capability –the concept

NEC Delivery Project Team[1]

Anthony Alston
QinetiQ Ltd

Abstract
The key to Network Enabled Capability is the ability to collect, assemble and disseminate accurate, timely and relevant information faster to help to provide a common understanding among commanders at all levels. Research is being carried out to examine how implementing NEC affects the procurement of equipment. The author describes the team's initial findings.

Meeting the aspirations for NEC will require hard decisions to be made on the balance between core capability, net ready (capabilities necessary for participating in a wider network community) and altruistic needs (those beyond core requirements for the greater good of the network), without which a networked force cannot be achieved. The NEC conceptual framework derived in the paper provides a useful way of encapsulating the essence of what NEC is and what it is trying to achieve. However, to understand the impact of NEC fully, and its description in terms of the conceptual framework, requires stepping from the conceptual world into the practical one. This includes in particular understanding the impact on equipment acquisition and the metrics required to support it.

BACKGROUND

Following the success of the concepts behind the US Network Centric Warfare (NCW) programme [1], the MoD has stated that networked capability is to be core to the definition and operation of its future equipment capability. Implementing this initiative is called Network Enabled Capability (NEC).

The importance of NEC is shown by these comments from the Secretary of State for Defence and DCDS(EC):

> *'(NEC).encompasses the elements required to deliver controlled and precise military effect rapidly and reliably. At its heart are three elements: sensors (to gather information); a network (to fuse, communicate and exploit the information); and strike assets to deliver military effect. The key is the ability to collect, fuse and disseminate accurate, timely and relevant information with much greater rapidity (sometimes only a matter of minutes or even in 'real time') to help provide a common understanding among commanders at all levels'.* [2]

> *'To identify and prioritise the equipment capabilities required across Defence to enable the UK to develop a network centric/network enabled capability. This will include a 'model' that will enable the JCB and DECs to understand how projects 'fit into' the total Defence capability (on which I have already spoken to DEC CCII and CCII CBM)."* [3]

NEC is built on many of the same principles as NCW: future military operations will benefit from an environment in which

- information is shared
- all users are aware of others' perceptions of the battlespace (including an understanding of the commander's intent)
- decisions are based on collaborative discussion
- effects in the battlespace are synchronized.

THE UK NEC INITIATIVE

NCW is a formal US networking concept and doctrine directed towards a fully-fledged warfighting capability. It is at the heart of the US transformation process and has been described as "The embodiment of the information age transformation of the DoD" [2].

NEC shares the tenets of NCW but is more limited in scope in that it is not a doctrine or vision. Nor does it seek to place the network at the centre of capability in the doctrinal way that the term NCW implies. Rather, NEC is much more concerned with evolving capability by providing a coherent framework to link sensors, decision makers and weapon systems to enable emerging UK doctrine (from JDCC) on effects-based operations to be achieved. The term NEC also implies the wider value of networking across the spectrum of operations, and not solely war fighting. Figure 1 shows this.

A research programme led by Dstl[4] is aimed at defining what NEC is and assessing the impact on the lines of development[5] required to achieve it. In particular, the

1 The delivery team is led by *Dstl, and supported by QinetiQ and others.* Anthony Alston is the lead author for this paper.
2 Secretary of State for Defence, Strategic Defence Review New Chapter, July 2002
3 DCDS(EC) –Air Marshall Sir Jock Stirrup, April 2002
4 NEC Delivery Project Manager, Jonathan Williams, Dstl.
5 The six lines of development cover all the aspects of military capability: structure and processes, concepts and doctrine, equipment capability, personnel, training, sustainment.

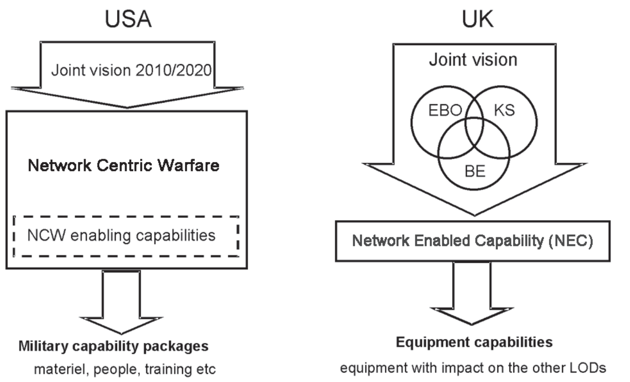


Fig 1. Comparison of NCW and NEC military aspirations

programme is tasked with defining the detailed impact on the equipment line. This paper presents some of the programme's initial findings.

MILITARY ASPIRATIONS

The world order has changed significantly over the last decade, and continues to do so. To adjust to this, the UK requires an agile and adaptable military capability that can be deployed globally to counter threats ranging from traditional attrition-style conflicts to those that are very asymmetric. The military aspirations for the UK Forces will provide the goal for which NEC will be a prime enabler. The military aspirations used to derive the NEC Conceptual Framework have been derived from the Joint Vision documents prepared by JDCC [3,4]. The aspirations are for a force that is:

Responsive –can respond to changes in need, matching tempo to the operational situation

Robust –remaining effective in the face of depletion of its resources or capabilities

Broad –able to operate effectively over a wide range of situations and missions

Flexible –capable of achieving effects in many ways, using agile resource groupings

Adaptable –learning from its operating environment and acting accordingly

Scalable –capable of operating in large or small deployments, minimizing its in-theatre footprint

Interoperable –operating jointly across all levels and with allies, OGDs and NGOs

Synchronized –Working coherently to deliver coordinated effects and avoid internal conflicts

Proactive –rapidly generating and deploying mission groups, and achieving aims quicker

Responsible –operating with minimal fratricide or unintended effects

Cost effective –delivering effective military capability at lower cost.

NEC REALIZATION CONCEPT

An aspirational statement describing NEC is required to put the military aspirations into a context suitable for NEC to be realized. To this end, CM(IS)[6] has provided a high-level mission statement for NEC:

> *'NEC allows platforms and C2 capabilities to exploit shared awareness and collaborative planning, to communicate and understand command intent, and to enable seamless battlespace management. It will underpin decision superiority and the delivery of rapid and synchronized effects in the joint and multi-national battlespace."*

To achieve these aspirations will require a shift in how systems, in the broadest socio-technical sense, are defined. In the past, platform-centric thinking provided systems to accomplish independently defined tasks, in isolation of how they would interoperate with other systems. This provided optimal systems that performed poorly when operated with others. This led to an evolution in thinking, resulting in integrated systems. Here, individual systems were considered in the context of how they joined with others to perform larger, end-to-end, operational missions. This led to optimal configurations able to perform one, or a few, missions very well. This was fine in the Cold War era where the threat was well understood. In the changing world of the 21st century, the military require a flexibility that integrated systems cannot provide. Network-centric thinking takes integration one step further by providing a 'network' through which the systems interact without prescription. This meets the need, set out by CM(IS) above, for enabling platforms and C2 capabilities to exploit each others' capabilities rapidly and flexibly in ways not originally envisaged when designed. This evolution in thinking is shown in figure 2.

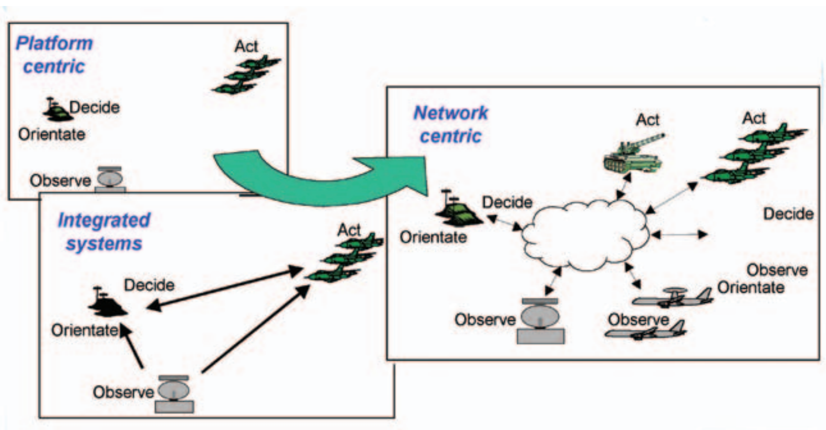


Fig 2. Evolution from platform to network-centric thinking

6 Major General Rob Fulton, Capability Manager Information Superiority CM(IS), 30 April 2002.

To deliver this network-centric vision, and to realize the military aspirations listed earlier, it is necessary to consider the vision in the context of some real-world constraints, including the following:

In the operational battlespace, there will be no underlying infrastructure for deployed assets to 'plug into'; ie, there is no independent 'network' for assets to join. The deployed assets themselves will be the nodes of the network and hence will include 'network' functionality above and beyond that functionality required of them for their operational roles. The network functionality resident within a particular asset will be dependent on the role of the asset and the potential altruistic role it could perform for the wider operational community. The definition of the Global Information Infrastructure (GII) and the delivery of the infrastructure will play crucial parts in the definition of network functionality.

An asset's interoperability will be defined in terms of its role as a network node and its operational role. In its operational role, interoperability splits into two: technical interoperability and co-operability. Technical interoperability is its ability to 'network' with assets at a technical level; co-operability is its ability to work with other assets to support an operational mission. Co-operability will be defined by the 'communities' with which an asset may wish to participate –for example, Time-Sensitive Targeting missions or collaborative operational-level planning. However, to avoid restricting the flexibility of an asset, there will need to be a base level of co-operability that all assets can achieve.

What an asset must do to become part of the network and to interoperate and co-operate with other users in the battlespace can be regarded as the definition of 'Net Ready' for that asset.

Resources may be scarce in the future battlespace, and hence will need to be better utilized than at present. This will mean, amongst other things, that assets must be able to be shared between mission and mission types, dependent upon their availability.

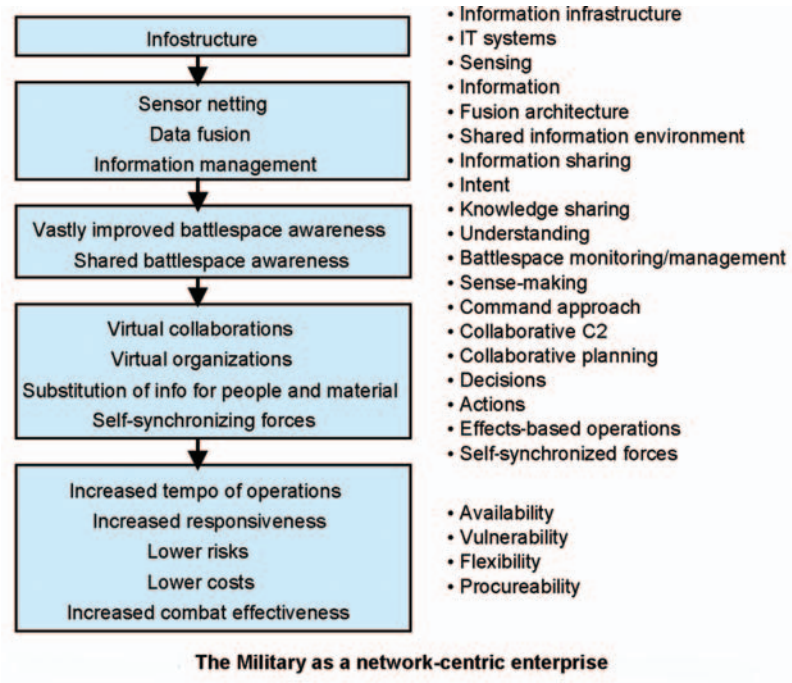


Fig 3. Enablers of network-centricity

THE NEC THEMES

The definition of NEC stemmed from the enablers required to meet the aspirations of network-centric thinking. The diagram of the military as a network-centric enterprise [5] was used as a starting point. This was expanded upon to identify the enablers of network centricity, some of which are shown in figure 3.

The list of enablers was large and required grouping to enable the definition of NEC to be simplified to manageable proportions. This grouping resulted in the NEC themes, which define the essence of what NEC is across the six lines of development. Initial analysis of NEC identified a large number of capabilities ranging from sensor exploitation, through collaborative planning to synchronized effects. Grouping these capabilities leads to nine themes; eight of these cover equipment capability and one the acquisition process (see table 1).

Table 1
NEC themes

Agile mission groups	Enabling the dynamic creation and configuration of mission groups that share awareness and that coordinate and employ a wide range of systems for a specific mission
Fully networked support	Allowing the ready use of non-frontline government bodies, industry, academia and public service capabilities to support operations
Flexible working	Enabling assets to rapidly reconfigure to meet changing mission needs, allowing them to work together with minimum disruption and confusion
Synchronized effects	Achieving overwhelming effects within and between mission groups by coordinating the most appropriate assets available in the battlespace through dynamic distributed planning and execution
Effects-based planning	Taking an approach to planning that focuses on the use of military and non-military effects required against an enemy, and is integrated with other planning processes in the battlespace
Shared awareness	Providing a shared understanding and interpretation of a situation, the intentions of friendly forces, and the potential courses of action amongst all elements in the battlespace
Full information availability	Enabling a user to search, manipulate and exchange information of different classifications captured by, or available in, all sources internal and external to the battlespace
Resilient information infrastructure	Ensuring information resources can be managed and that secure and assured access is provided with the flexibility to meet the needs of agile mission groups
Inclusive flexible acquisition	Coordinating process across MoD, OGDs and industry that promotes the rapid insertion of new technologies, facilitates coherence between acquisition programmes and provides an incremental approach to delivering 'net-ready platforms'

Throughout the analysis of the enablers, there was the common thread of information; not just getting the right information to the right place at the right time but *using it better* when it got to the destination. The importance of this, which is perhaps one of the critical differentiators from previous initiatives such as JBD, is reflected in the NEC themes. Only three –resilient information infrastructure, full information access and shared awareness –are about moving information; the rest are about using it better.

Agile mission groups
The formation of network-centric forces must not be constrained by hard-wired equipment configurations based on organizational structures. The network-centric force will be composed of capability components brought together to form ***agile mission groups*** to undertake specific operational tasks. The tasks may be long-lasting, for example protection of an air-head, or transient, for example destruction of a communications mast. Once complete, the elements of the agile mission group will return to their host functionally or environmentally oriented organization. Shared awareness in an agile mission group will need to be very high for understanding and achieving the common goal, but lower between it and other agile mission groups, where a general understanding of the intent or position may be all that is required. The high level of shared awareness will require elements of agile mission groups to have correspondingly high levels of 'application interworking' to ensure the synchronization of planning, control and effects. The concept of 'asymmetric collaborative working' [7] makes attaining a high level of application interworking complex. This concept recognizes that capability components in an agile mission group may have very different levels of IT support (or indeed training and expertise): for example, an agile mission group composed of dismounted infantrymen or headquarters-based users. This requires an interworking regime that can cope with different levels of capability.

Fully networked support
The membership of operational forces, including agile mission groups, should not be restricted to the in-theatre forces but will include non-frontline government bodies, academia, industry and public services. Hence, a dynamic resourcing mechanism is required that makes use of such capabilities to support the in-theatre capability, for example logistics, data/image analysis and medical support.

Flexible working
Agile mission groups will be how network centric forces exert effect in the battlespace. Ideally, agile mission groups will be made up from elements suited to their allotted roles. However, this will not always be possible. Elements will need the flexibility to:

- undertake tasks not supported by their primary roles
- work with other elements with whom they have not previously been expected to work
- work in several agile mission groups simultaneously, maintaining coherent situational representation between the agile mission groups and not compromising their roles in any of the groups
- be able to change rapidly from one agile mission group to another without disrupting the operation of either group.

Synchronized effects
An efficient, effective dynamic planning and C2 system is a key element of NEC, and is vital to coordinating the many diverse strands of operations to achieve synchronicity. Without it, planning and managing a number of complex tasks with different tempos simultaneously, and making dynamic use of resources, will not be feasible. Success will require breaking down the barriers within command and control and exercising it as a single process; the hard distinction between planning and execution must be broken down and replaced by a single dynamic planning, tasking and execution process, thereby increasing tempo and responsiveness. The battlespace will contain many separate planning teams, who themselves could be distributed, and their planning processes must be synchronized, thereby creating a more synchronized force. The coordination between the planning groups will include the coordinated use of the battlespace environment, which encompasses such diverse elements as airspace, waterspace and RF spectrum. This coordination is done as part of command management.

Effects-based planning
Network centric forces will have access to many other effectors in the battlespace above and beyond the traditional 'attrition' effectors. In particular, information operations, considered currently as a separate, stand-alone capability, should be brought into the mainstream of military planning and execution, thereby being treated as just another battlespace effector and hence providing more operational scope to the battlespace commander. To utilize all these effectors fully, operational planning will have to change from an attrition-based process to an effects-based one. The following are required to allow the full scope of effects-based planning (EBP) and effects-based operations (EBO):

- A fully capable EBP capability, operational through all levels in the MoD and in all other government departments that influence political/military/economic aims (including Foreign Office, Home Office and Treasury). In the MoD (and potentially elsewhere), this capability will have to be able to operate with the dynamic, distributed planning systems required for the delivery of synchronized effects and the management of agile mission groups.
- Modelling tools that permit prediction and questioning across the whole domain of EBO, including predicting the interaction between military, diplomatic and financial effects.

7 Asymmetric collaborative interworking is a term coined by Dr Martin Young of QinetiQ.

- Tools to assess the effects of operations across all domains. These will expand on traditional BDA tools for assessing military effects, capitalizing on the greater sharing of information to allow more rapid/simultaneous assessment, and adding assessment of the effects in non-military domains (political and economic).

Shared awareness
This is a central facet of NEC and underpins many of the other themes, including agile mission groups, synchronized effects and effects-based planning. Achieving awareness is a cognitive activity that results in a gaining of a personal understanding of what is happening, and of why and what could happen in the battlespace. Gaining understanding requires appropriate processes and training as well as supporting equipment. Shared awareness, in the context of NEC[8], is the ability to communicate an individual's understanding to others in order that, as a group, there is some level of shared understanding. Shared awareness has two principal elements.

> ***The gathering, maintenance and presentation of relevant information.*** This will include extracting information from all relevant, available sources (including coalition partners, OGDs and NGOs as appropriate), seeking specific additional information and/or clarification, and combining all this information to produce a local representation or 'picture' that meets an individual user's needs. However, shared awareness will only be supported if separate local 'pictures' are self-consistent. The goal for NEC is a set of consistent pictures across the battlespace rather than a common one. This approach is aligned with the concept of a Joint Operations Picture (JOP) [6] defined as:
>
> *'The total set of shared information on a particular operation, or Joint Operations Area, available through a secure information environment on operational CIS networks to support situational awareness and decision-making by UK commanders, and to facilitate information sharing with allies and partners in Joint and multinational operations."*
>
> ***Developing a shared understanding of the situation.*** Understanding exists not in the underlying information gathered from across the battlespace but in the mind of the user. To achieve a common shared awareness, the understanding must be communicated to others. If the users are collocated, verbal and non-verbal (body language) means can and are used. If the users are distributed, equipment must be used to support the 'encoding of understanding' and of its transmission. The equipment could attempt to replicate collocation, for example video teleconferencing, or could encode understanding for presentation on standard IT equipment, for example using text and graphics.

8 The authors appreciate that this does not match the academic definition of shared awareness. Strictly speaking, awareness cannot be shared; it is an individual's understanding, gained from awareness, that can be shared.

Full information availability
The future battlespace will be teeming with information. NEC will make much of this information available to users. This will include access to the widest range of information sources, including military (ISTAR, intelligence sensors, weapons sensors, etc), civil (news feeds, environmental information, etc), encyclopaedic information, archived information, information available from sensors of opportunity and information collected but not fully exploited. However, this does not mean that all this information will be pushed to the user, overwhelming him with irrelevant information. On the contrary, only a very small part of this information pool will be presented to any user (for example, orders, plans and predefined information needs). The user, or application, will have to search for the rest of the information actively from across and beyond the battlespace. To facilitate this, the user, software application or system will be provided with the capability, tools and mechanisms to proactively, rather than reactively, search for, manipulate and exchange information. The capability must allow the searching and exchanging to take place not only within national systems but also across those of coalition partners and the Internet. This will require the tools and mechanisms to handle data of different classifications securely. In summary, this proactive searching mechanism must be an adjunct to, not a replacement for, other information management mechanisms such as selected information push and broadcast, providing the user with a rich set of information access and retrieval mechanisms.

Resilient information infrastructure
Such an infrastructure is required to provide a secure and assured environment to meet the requirements of a dynamic battlespace equipment capability, and in particular the demanding, dynamic requirements of agile mission groups. Many of the aspirations of the resilient information infrastructure theme are captured by the GII concept. The requirements include:

- the capability to share information across the battlespace, and allow all users (human or machine) access to the information needed for planning, executing and monitoring operations. This capability should allow information to flow transparently across domains, be robust in the face of communications limitations and ECM, and should support the information user (human or machine).

- efficient management of information sharing, as demanded by the operational situation, and the requirements for information access

- the provision of an assured end-to-end performance based upon the business need.

Inclusive flexible acquisition
The equipment acquisition process must cater for the aspirations of NEC, whose requirements range from a more coordinated approach to defining equipment capability to a holistic view of the equipment programme –the relationship

between individual acquisitions and the delivery of coherent packages of military capability. Of prime importance in a domain where the fundamental technology is evolving rapidly is the ability to take advantage of new technology. Exploitation of leading edge technology will otherwise be impossible[9].

NEC EQUIPMENT ACQUISITION CONTEXT

Equipment to support the aspirations for NEC will be provided by the MoD's current equipment acquisition process, Smart Acquisition [7], where systems are acquired by independent projects to meet their own set of user requirements within established time and funding limits. As currently envisaged, there will not be any NEC projects; the aspirations for NEC will only be met through the combined effects of many of these independently specified and procured systems. This requires, as a minimum, additional NEC requirements to be placed on contributing systems above and beyond those required to meet their core purpose. The challenge is how to specify NEC requirements on each of the contributing systems to ensure that the desired NEC capability results when they are brought together as a system of systems.

Much work has been done to determine the nature and behaviour of a system of systems, primarily in a MoD context. Particular attention has been paid to performance and to how this should be specified and acquired [8,9,10]. Two major conclusions are directly relevant to NEC:

- a large system-of-systems cannot be defined top-down; that is, derived in a hierarchical fashion from a single statement of requirement. Many now believe that system-of-systems behaviour is an emergent property of bringing together individually acquired systems and that these emergent properties cannot be 'designed in' to each component part.

- each equipment in the system-of-systems has a number of stakeholders with their own, often conflicting, requirements. NEC will provide yet another set of requirements that will need to be balanced and traded.

The consequence for NEC is that it will provide requirements to some, if not all, equipment acquisition programmes through the entirety of their lifecycles (see figure 4). In fact, NEC demands careful maintenance of equipment capability through the coordination, specification and prioritization of individual equipment programmes. Four areas of influence have been identified [11]:

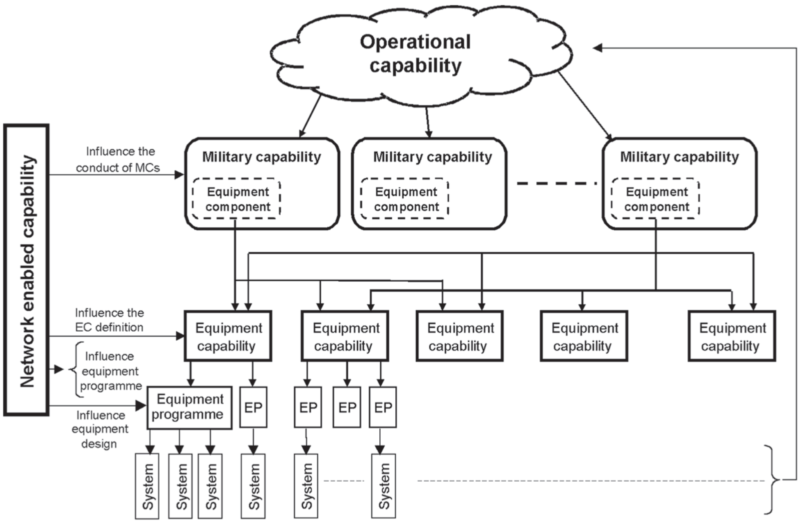


Fig 4. Integration of NEC capability requirements

Conduct of the military capabilities

NEC will greatly affect how military capability is achieved. This effect will range from the enhancement of current capabilities, such as time-sensitive targeting, to the total redefinition of what military capability is. This starting statement of military capability in terms of NEC will provide a sound footing for the development of the six lines of development that shape overall military capability.

Definition of equipment capability

NEC will have the opportunity to influence the definition of equipment capability directly, which will already have been specified in terms of the support provided to a number of military capabilities. The influence on equipment capability definition could be through the insertion of new NEC-based user requirements but will be more likely to be by coordinating user requirements definitions across the equipment capabilities to ensure conformity to the principles of NEC.

Equipment design

To achieve the aspirations of NEC, it will not be enough simply to align the user requirements: the implementation must also be aligned. This may be done through such mechanisms as the JSP 602 leaflets but primarily by influencing infrastructure projects such as the DII.

Equipment programme

The equipment component of military capability will be made up from many systems, procured independently to different timescales. NEC will ensure that appropriate programmes are linked and prioritized to deliver coherent support to military capability.

If NEC is to be achieved, its influence on equipment acquisition must be given a high priority if it is not to be traded-out in the usual cost and requirements balancing process.

In this way, NEC will provide a framework against which military capability will be defined and equipment capability acquired [11]. At the core are the NEC themes and the conceptual framework.

9 This theme is further addressed in the paper 'Can NEC be delivered?' page 160 of this issue.

NEC CONCEPTUAL FRAMEWORK

The NEC themes have been derived from analysing what NEC will enable within the battlespace. Hence they only cover the NEC-related aspects of the lines of development. This means they cannot be used to define any of the lines of development in a top-down manner. Rather, they should be used by developers in the lines of development as a 'style', or the operating context, within which particular areas should be considered.

Figures 5 and 6 show how this style could be applied to the analysis of a component of military capability. Figure 5 shows a generic layered model of a component of military capability (the remainder of this section uses 'an offensive air capability' as an example of a component of military capability):

The fundamental elements are the military 'task' and the 'capability component' to provide it. These could be the range of target types and a description of the capability to counter them.

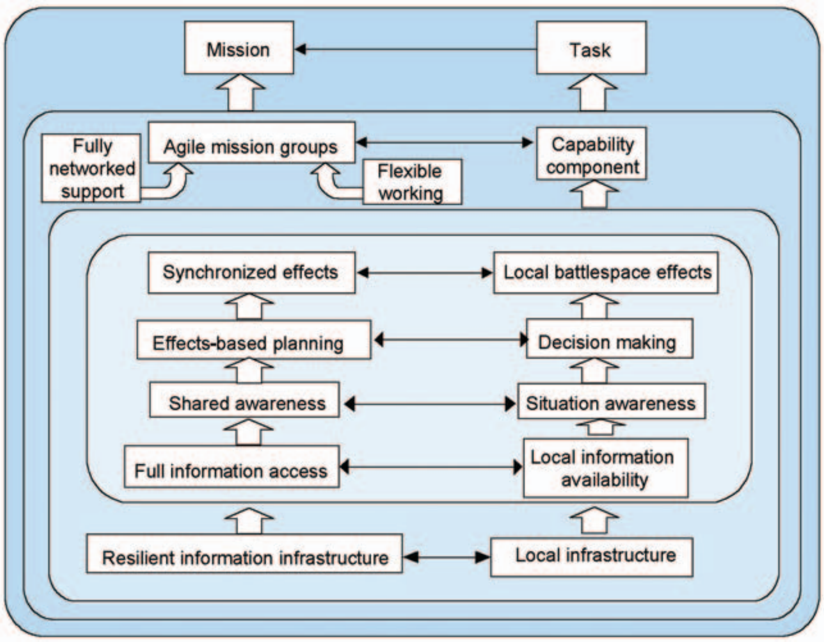


Fig 6. The NEC conceptual framework

The capability component has a local infrastructure, which could be an airframe, sensors and weapons systems all connected via Mil Std 1553b databus.

The local infrastructure supports the aircrew in gaining situation awareness from information derived from their local information sources (sensors).

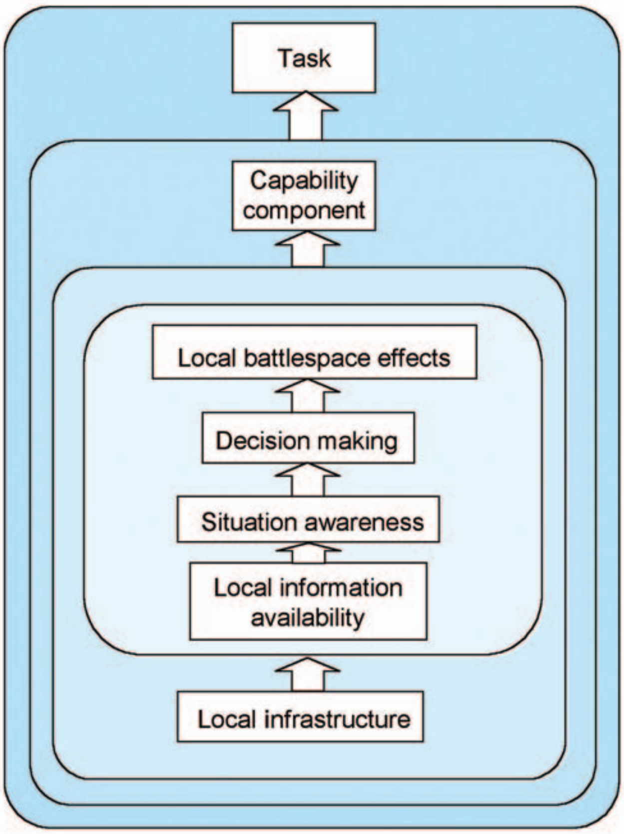


Fig 5. Conceptual framework for stand-alone capability component

Lastly, having gained situation awareness, the aircrew will require decision-making support to create local battlespace effects (fire their weapons).

Figure 6 shows how each step could be considered in the context of the NEC themes:

The task must be considered in the context of a larger mission within a range of specified scenarios.

The capability component must be considered in terms of agile mission groups, of which it will be a part. Fully networked support will provide a global context for the agile mission group (reach-back), while flexible working will provide the context for the capability component operating in more than one agile mission group at one time. This analysis will identify the interoperability requirements for the capability component.

The local infrastructure must be considered in the context of the resilient information infrastructure. This will identify infrastructure services that are available from the wider battlespace and those services that the local infrastructure could provide to other users. Local information availability must be considered in the context of full information access. Thus the aircrew are no longer constrained to information from local sensors but can benefit from information elsewhere in the battlespace. In return, local sensor information is made available to the wider community.

Situation awareness must be considered in the context of shared awareness. The aircrews' own situation awareness will be heightened by assimilation of others' awareness and understanding of the situation, and vice versa.

Decision making must be considered in the context of effects-based planning. How do aircrews' decisions affect or how are they affected by other decisions in the battlespace?

Local battlespace effects must be considered in the context of synchronized effects. How do effects caused by local weapon systems affect or become affected by other effectors in the battlespace?

NET READY AND ALTRUISTIC CAPABILITY

The objective of these diagrams is to demonstrate how NEC will influence defining capability components. There will not be an NEC definition that capability components will add to their definition; rather, they will define the capability component in terms of NEC. Hence, the NEC-related requirements taken on by a capability component are unique to that component and can only be derived through an understanding of the role of that component. Understanding the role of a capability component in the context of NEC leads to the identification of three types of capability needs (figure 7).

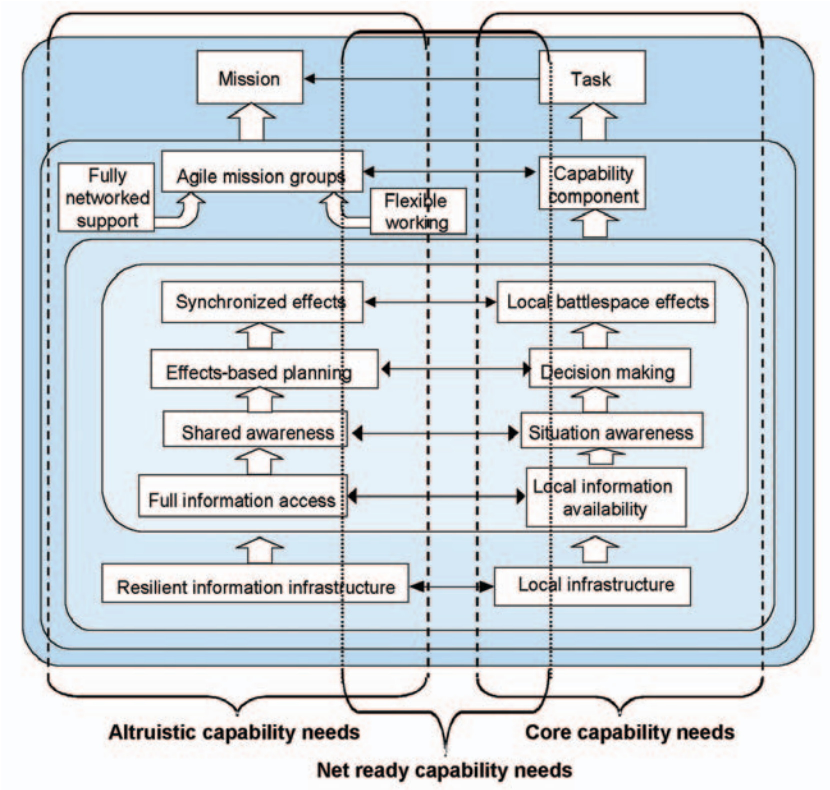


Fig 7. The three types of capability need

Core capability needs

These are required to meet the operational function of the system or platform. They are the reason that this platform or system is being acquired.

Net ready capability needs

The needs a capability must take on if it is to be able to participate as a member of the wider network community. These needs will augment and enhance a system or platform's core capability needs.

Altruistic capability needs

These are placed on a platform or system for the greater good of the network but they in no way enhance the capability of that platform or system in the context of its core capability need. An example of this may be additional communications capability with accompanying communications relay.

Three very important issues result from this analysis:

- only the host capability can define what it means for it to be net ready; an independent NEC body cannot do this
- the altruistic needs that are placed on a platform or system can only be derived through analysis of the requirements of the whole network
- The three sets of needs –core capability, net ready and altruistic –must be treated as a single set by the platform or system. All solutions must treat the needs as a holistic set.

Whilst the requirements associated with being net ready cannot be supplied by an independent NEC body, coordination across capabilities is required to ensure that all definitions of net ready and altruism are consistent. This can and should be done by an independent body.

CONCLUSIONS

The current work on NEC has shown that the aspirations for NEC can only be achieved through all the lines of development. In particular, in the equipment line, there is a clear need for coordination of platform and system definition, and acquisition. This will require hard decisions to be made regarding the balance between core capability, net ready and altruistic needs, without which a networked force cannot be achieved.

Much work still needs to be done on defining NEC. However, the NEC conceptual framework provides a useful way of encapsulating the essence of what NEC is and what it is trying to achieve. It can be used as the basis for describing other views of NEC – for example, defining how NEC affects the lines of development [12].

To understand the impact of NEC fully, and its description in terms of the conceptual framework, requires an understanding of how to take NEC out of the 'conceptual world' and into the practical one. This includes understanding the impact on equipment acquisition and the metrics required to support it [11,13], and work on NEC speculative architectures and their effects on concepts such as the GII [14].

Acknowledgement

The research was supported by the Ministry of Defence.

Glossary

BE	Battlespace Exploitation
C2	Command and Control
CCII CBM	Command and Control and Information Infrastructure, Command and Battlespace Management
CM(IS)	Capability Manager (Information Superiority)

DCDS (EC)	Deputy Chief of the Defence Staffs (Equipment Capability)
DEC (CCII)	Director, Equipment Capability (Command and Control and Information Infrastructure)
DII	Defence Information Infrastructure
DoD	Department of Defense
EBO	Effects Based Operations
EBP	Effects Based Planning
GII	Global Information Infrastructure
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JBD	Joint Battlespace Digitization
JCB	Joint Capabilities Board
JDCC	Joint Doctrine and Concepts Centre
JOP	Joint Operations Picture
JSP	Joint Services Publication
KS	Knowledge Superiority
Mil Std	Military Standard
NGO	Non-Governmental Organizations
OGD	Other Government Departments

References

1 Alberts D S, Garstka J J, Hayes R E and Signori D A. *Understanding Information Age Warfare*. Command and Control Research Programme (CCRP) (2001).

2 DoD Report to Congress on NCW (July 2001).

3 The UK Joint Vision. JDCC, D/JDCC/7/11/1 (15 June 2001).

4 A concept for effects-based operations. JDCC (20 May 2002).

5 Alberts D S, GartskaJ J and Stein F P. *Network Centric Warfare*. CCRP (1999).

6 UK Policy for the Joint Operations Picture, D/DJW/CBM/40/3 (4 July 2002).

7 The Acquisition Handbook – Version 4, Ministry of Defence UK (2002).

8 Taylor R. *Analysis methods for achieving desired emergent properties in a complex system of systems.* QinetiQ/KI/SEB/CRO20597 (March 2002).

9 *Joint Battlespace Digitization system integration architecture high-level user requirements document.* DERA and industry 'rainbow' team, DERA/LSB1/CR990305/0.2 (July 1999).

10 *Exploratory study of the systems integration architecture for Joint Battlespace Digitization*. DERA and industry 'rainbow' team, DERA/CIS/C153/CR990255/1.0 (July 1999).

11 *NEC Acquisition and Delivery*. Issue 2, Dstl/IMD/SOS/500/2 (28 March 2003).

12 *Impact on the lines of development.* Issue 1, Dstl/IMD/SOS/500/2 (March 2003).

13 McInerney S and Montgomery J. *Metrics for network enabled capability.* Dstl/CR05743/1.0 (January 2003).

14 *Speculative architectures*. Dstl/IMD/SOS/500/2, Issue 1.0 (March 2003).

Dstl Portsdown West, Portsdown Hill Road, Fareham, Hants PO17 6AD
jpwilliams@mail.dstl.gov.uk

Network Centric Warfare: current status and way ahead

David S Alberts
US Department of Defense

Abstract
The US Department of Defense is committed to transformation, a transformation that, in large part, involves both the adoption of and adaptation to Information Age technologies. In the final analysis, the success of our efforts at transformation will be directly related to our ability to bring information to bear in our warfighting and other national security missions as well as in the business processes necessary to acquire capabilities and support operations. Network Centric Warfare is the embodiment of the information age in the domain of warfighting, and, as such, is central to defense transformation. Given that no significant military action is conceivable without the need to form a coalition, it is important that progress both here and abroad towards both an understanding of NCW and the achievement of NCW-related capabilities be measured, assessed and facilitated. This article represents a personal view of the progress made to date and the steps needed to ensure continued progress from this point on.

UNDERSTANDING NETWORK CENTRIC WARFARE

Network Centric Warfare was not born in a fully developed form but, as is the case with most truly innovative ideas, has developed to its current state as the result of an on-going dialogue among its early and more recent and increasingly diverse proponents. No one, not even the authors of the most widely read book on the subject[1], can speak with final authority on NCW orthodoxy. NCW is, and will continue to be, a product of many fathers, many of whom are at this point in time, unborn. Therefore, this article represents, of necessity, just one individual's view. It is, however, the view of an early proponent, the author of a number of books and reports related to NCW[2], and one who is involved in working with others on a day-to-day basis to realize the promise of NCW.

The logic of Network Centric Warfare is most succinctly expressed by the tenets depicted in figure 1.

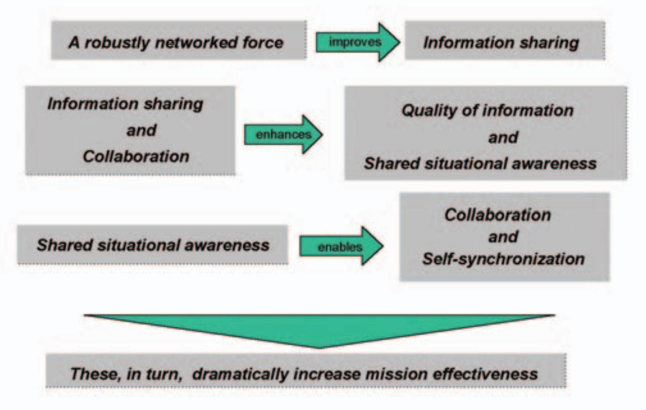


Fig 1 Tenets of NCW

It has been said, and correctly so, that the entry fee to NCW and the Information Age is a ***robustly networked force.*** This cannot be achieved without a ubiquitous, secure, robust, trusted, protected and routinely used wide-bandwidth net that is populated with the information and information services that military forces need. However, for too many people, this is not only where NCW begins: it is where it ends for them – with a laser-like focus on technology. NCW is so much more.

The real magic of NCW lies in the leap that occurs between the achievement of ***shared situational awareness*** and ***collaboration and self-synchronization.*** And like most 'magic' it does not take place by accident, rather it is the result of a lot of study and hard work. What lies at the heart of the matter is the co-evolution of concepts of operation, organizations and approaches to command and control with advances in technology. Thus, Network Centric Warfare traverses four domains: the physical, information, cognitive and social[3], and is a reflection of the synergies among these domains. Proceeding with an insertion of information technology that improves the infostructure does not even move us one rung up the NCW ladder. Quite the contrary, it may have adverse consequences[4].

Network Centric Warfare is not an all or nothing proposition. Put another way, it is not a destination but a journey. Forces can be more or less network-centric with their effectiveness, according to the theory, linked to their degree

---

[1] The most widely read book on NCW is Alberts, Garstka and Stein's *Network Centric Warfare: Developing and Leveraging Information Superiority,* published by the US Department of Defense Command and Control Research Program (CCRP) available at www.dodccrp.org. The authors make this very point on page 5 in the section on NCW Myths.

[2] These include roles as either the author or co-author of: *Understanding Information Age Warfare*, *Information Age Transformation*, the *NCW Report to the Congress*, and a recently published book *Power to the Edge: Command and Control in the Information Age,* available at www.dodccrp.org.

[3] *Understanding Information Age Warfare* discussed the first three of these domains. A joint research effort sponsored by the CCRP and the US Office of Force Transformation has developed an initial conceptual framework for NCW that adds the fourth (social) domain.

[4] This is explained in the books *Unintended Consequences of Information Age Technologies* and *Information Age Transformation.*

of network-centricity. To characterize degrees of the achievement of NCW, a maturity or capability model was developed[5]. This model is shown in figure 2.

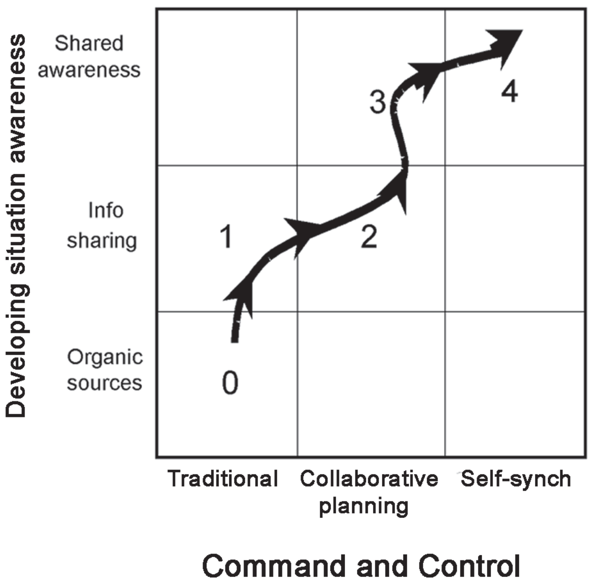


Fig 2 NCW levels of maturity

Thus, while achieving a robustly networked force is necessary to achieving 'full' NCW capability, progress can be made in increments. For progress to be made, however, concurrent changes need to be made to the way individuals and organizations think about and handle information. To get to Level 1 for example, individuals and organizations must not only be able to share information but they must also be willing to share it. For the most part, existing infostructures are more capable of sharing information than the extent to which information is actually shared. Furthermore, commercially available technologies can significantly improve most military infostructures. Therefore, a great deal of progress toward higher levels of NCW capability can be achieved with little or no new investment in technology. Instead, what are needed are investments in education and cultural change.

In essence, NCW is all about moving ***power to the edge***[6]. It is about changes to our organizational processes and behaviours. A key to moving power to the edge is providing all individuals and organizations with timely access to the information they need and the capability to participate in collaborative processes. A recent report to the Congress stated that NCW is the embodiment of an Information Age transformation of DoD and that it will involve a new way of thinking about how we accomplish our missions, how we organize and interrelate, and how we acquire and field the systems that support us[7]. ***Power to the Edge*** is the principle that is guiding us in the US DoD in rethinking our policies, organizations and processes.

As indicated earlier, Network Centric Warfare is predicated upon the ability to create and share a high level of awareness and to leverage this shared awareness to self-synchronize effects rapidly. Awareness takes place in the cognitive domain and thus is much more than simply about what information is available. The tenets of NCW contain the hypothesis that sharing information and collaborating with others about the meaning of the information improves both the quality of the information and the quality of the awareness that results. Thus it is the interaction of changes in the information, cognitive and social domains that are needed to move from Level 1 to Level 2. Achieving shared awareness (at Level 3) will allow us to bring all of the available information to bear. Moving to Level 4, which involves the 'magic' of NCW, will permit us to bring all of our assets to bear as well, greatly increasing combat power. This leap to self-synchronization primarily involves changes in the cognitive and social domains.

Success requires that we think about information, command and control differently. In the information domain, we need to move from a set of monopoly suppliers of information to an information market-place. Only by doing so will we be able to ensure that our forces will have the variety of views and perspectives necessary to make sense out of the complex situations they will face. And only by moving to market-places can we ensure that our information collection and analysis capabilities will dynamically evolve to changing circumstances. Similarly, we need to move rapidly from a push-oriented dissemination process to a pull-oriented one. This is the only way to satisfy the needs of a heterogeneous population of information users.

Our approach to interoperability needs to change as well. Given the rate of advancing technology, we need to move from an approach based upon application standards to one based upon data standards. We need to give users of information the opportunity to use the applications that make sense to them while maintaining the ability to exchange information. Finally, we need to pay a great deal more attention to supporting peer-to-peer relationships, and information exchanges that transcend individual systems and organizations. Doing these things will empower the edge of the organization and enable us to change the way we approach command and control, particularly the way we exercise control. Command will evolve into a more collaborative process that selects from a set of alternatives developed and presented from the edge rather than options generated by a centralized planning process. Control will move from a set of constraints to an emergent property of the force.

NCW involves an historic shift in the centre of gravity from platforms to the network. In NCW, the single greatest contributor to combat power is the network itself. However, it will be moving ***power to the edge*** that will multiply the power that can be generated from a given set of assets and available information. All force entities will be able to generate

[5] This model was developed during the writing of *Understanding Information Age Warfare* (and is also contained in the *NCW Report to the Congress.*

[6] "Power to the Edge" is the current tag line for the vision statement of the US Assistant Secretary of Defense (Command, Control, Communication and Intelligence).

[7] NCW Report to Congress –Executive Summary

more power individually and in concert with other entities when they are connected to the net and can contribute information and expertise to it. The marginal value of an unconnected platform pales in comparison to the value it can generate if it is 'net ready'. The value of the current collection of disparate networks pales in comparison to the value that they can generate when connected to form a seamless infostructure. The net is needed to move ***power to the edge***. Moving ***power to the edge*** is the principle that will turn the theory of NCW into practice and result in military transformation.

STATUS AND WAY AHEAD

A great deal of progress has been made since the ideas that became known as Network Centric Warfare were first articulated. But, as the *NCW Report to the Congress* states[8], "Application to date of NCW theory has barely scratched the surface of what is possible." This characterization of progress will continue to reflect reality as long as the focus remains primarily on technology and not on the co-evolution of network-centric mission capability packages.

Having said that, proofs of concept of the power of NCW coming out of both real world experiences as recently as Afghanistan and Iraq and a variety of exercises and experiments[9] amply demonstrate that moving up the NCW capability ladder pays off handsomely. In other words, one gets payoffs all along the way to a fully mature set of NCW capabilities. The risk is that many will be satisfied with incremental improvements in competitiveness and not make the effort to reach fuller NCW capability. History shows that this behaviour can ultimately result in a strategic defeat. Thus, incremental gains achieved are best re-invested into the enterprise, with each success leading to increased efforts in infostructure and co-evolution.

The degrees to which the views of NCW expressed in this article are understood differ widely not only from country to country but from organization to organization and from individual to individual. There are individuals in many countries who understand the implications of the information age and share this vision. These individuals are as likely to be inside the military as they are to be in industry. NCW, in one form or another, is a major thrust in a number of countries including the United Kingdom, Sweden, The Netherlands, Denmark and Canada. As experiences with instantiations of NCW are shared, more will be learned, and more individuals will be convinced of its potential.

This internationalization of the understanding of NCW theory and practice is a necessary prerequisite for the ultimate NCW experience. That is, of course, network-centric coalition operations. Progress toward this goal depends upon coalition experimentation of the sort that has not been seen to date. The kind of experimentation that is needed involves collaborative discovery of the principles of information age command and control. These experiments will not be focused on technology, as many of the current and planned efforts are, but on mindsets and processes. The answers are not known or even knowable in advance but must be mutually discovered.

I have been asked repeatedly by individuals from many countries, 'What is the one thing we should do next?' This usually means what they should buy. If there were a 'correct' answer, it would clearly be different for each organization and each country because it would depend upon the state of their infostructure and the state of their minds. In many cases, it is not as much about what needs to be bought but what needs to be done to change mindsets. The current state of affairs cries more for leadership than for analysis. In order to move further down the road to NCW capability, a force must understand the vision and make the changes necessary in their expectations and relationships. It takes leadership to provide this understanding and to change the culture so that it is open to new command concepts that reflect a move to power to the edge.

[8] See page vii of the Executive Summary

[9] Many of which are documented in the NCW Report to Congress. The use of mounted Special Forces in connection with air power in Afghanistan represents a network-centric innovation that proved most effective. This was an interaction between ground and air forces that was not built into the specifications of the systems supporting them nor rooted in doctrine.

Director, Research and Strategic Planning, OASD(NII), Department of Defense, USA
David.Alberts@osd.mil

Testing the impact of NEC options on communications infrastructure and campaign outcome

Lynda Sharp and Brian Stewart
Policy and Capability Studies Department, Dstl

Abstract
Whatever the eventual impact of network enabled capability, its pursuit will necessarily change the demands for information at all levels of command compared with the way military business is carried out now. This in turn will stimulate changes in the way headquarters are organized and in the processes for planning and conducting operations. Elements of ISTAR and the way they are networked will be particular candidates for change. To explore how these changes could affect communications infrastructure, a method has been developed to test whether programmed capabilities in information and communication services will be able to meet the demands of future military operations. Effects have been addressed at two levels: first, at the communications network level, to examine the ability of planned networks to handle the demand for information arising from the conduct of future campaigns; secondly, at the campaign level, to compare the effects of investment in ICS and ISTAR with other investments in weapons and platforms. The authors conclude that, while further work will be necessary, for example to track emerging NEC concepts, the analytical method can help to inform decision makers on both issues.

INTRODUCTION

Network enabled capability will create changes in the demand for information compared with the demands of current ways of doing military business. For instance, it may lead to changes in the way headquarters are organized and in the processes followed for planning and conducting operations. In particular, it may change the way in which Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) assets are used and/or networked. Such change will modify the patterns of information flow around the battlespace in terms of the types of services required (video-conferencing, voice, data, etc), the priorities and frequency of information exchanges, and the connectivity needed to share awareness. A way is needed of testing the effect of these potential changes on the communications infrastructure, and of assessing their value to the overall campaign.

We describe a method that has been developed, and successfully applied over the past few years, to test the sufficiency of the UK's programmed capabilities in Information and Communication Services (ICS) to meet the demands placed upon them by ISTAR systems. The method measures the effects of ICS and ISTAR at two levels: the first is at the communications network level, in terms of the ability of planned networks to handle the demand for information arising from the conduct of future campaigns; the second is at the campaign level, where the effects of investment in ICS and ISTAR can be compared with alternative investments in weapons and platforms. Plans are now being developed to exploit this method, to test the impact of potential NEC concepts.

The method adopts a top-down approach by starting from consideration of an operation at the campaign level. It has four key steps (figure 1):

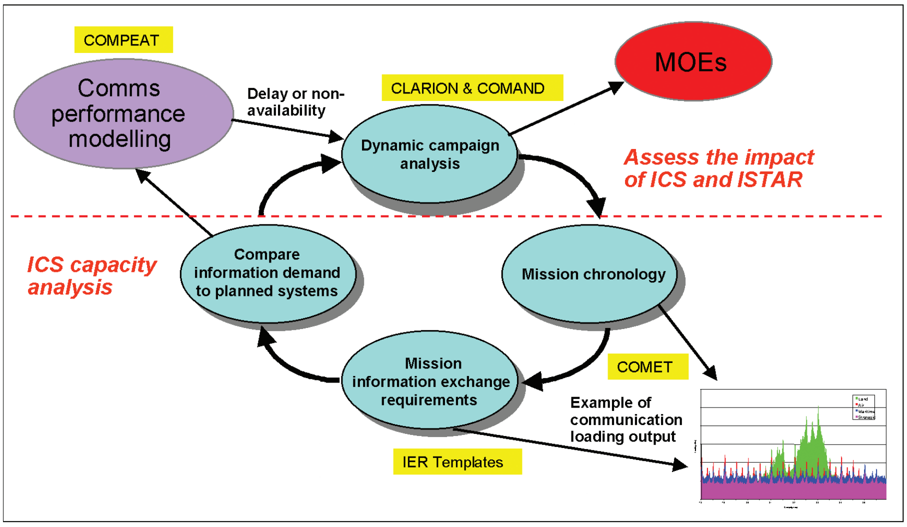


Fig 1. Outline of the method showing the key steps

- define the flow of activity in the campaign
- determine the demand for information arising during the campaign

- test the demand against the capabilities of planned communications infrastructures
- determine the effect on campaign-level measures of effectiveness.

For testing NEC concepts, this process would be conducted for a baseline campaign (based on current ways of doing military business) and then repeated for each NEC concept, to enable consequences at the network and campaign levels to be compared. The four steps are described next.

KEY STEPS

1 Defining the flow of activity in a campaign

The first step is the production of a campaign chronology that identifies the flow of missions over time by each of the participating force elements. Such a chronology is normally produced by extracting the detail from a run of one of the Dstl campaign models, CLARION[1] or COMAND[2]. The chronology provides a high-level view of 'who was doing what and when'. This is only possible because the models are command and control led, with identifiable missions at all command levels.

2 Determine the demand for information arising during the campaign

The next step is to estimate the information loading that would arise from the flow of missions. This is achieved through the use of Information Exchange Requirement (IER) templates for each type of campaign mission. An approach has been developed that starts by considering the business process involved in planning and executing the mission, and then identifying the information exchanges that would follow.

A baseline set of mission IER templates has been developed that is based on the current ways of doing business but with the removal of the technical constraints of current ICS services. Thus, whilst the processes reflect current concepts of operation and use, the medium assumed for the information exchange (video-conferencing, data, voice, or imagery) reflects the aspirations of the users. Each IER captures the source(s) and recipient(s), the reason for the exchange, the frequency with which it occurs per day, the preferred medium, the duration (for voice and video-conferencing) or size (for data and imagery) of the exchange, and the urgency.

The IERs have been developed with and reviewed by military staff, including those serving in relevant headquarters and units, involved in the conduct of each mission type. It is worth noting that the IERs in the mission templates cover all aspects of the operation: planning, intelligence, targeting, logistics, etc. They also cover the spectrum of activity in the joint domain from strategic to tactical levels.

1 CLARION (Combined Land-Air Representation of Integrated OperatioNs) is a high level, fast-running simulation of land/air combat at the campaign level that is driven by a command and control system.

2 COMAND (C3 Oriented Model of Air and Naval Domains) is a Monte Carlo simulation of joint and combined combat operations at the campaign level that is driven by a command and control system.

The individual mission templates are then combined with the chronology from the campaign to produce an estimate of the information demand over time. An example is shown at figure 2. The tool used is COMET[3].

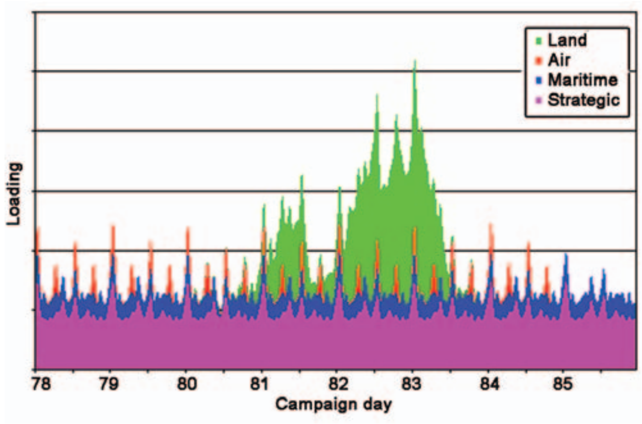


Fig 2. An example of the demand for campaign information with time

The baseline mission IER templates provide a framework against which NEC concepts can be compared. For each concept, alternative IER templates are produced that reflect the changed business process and resulting changes in information flows. Figure 3 shows the impact that two different NEC concepts might have on the pattern of demand for information services over the duration of a campaign. One of the expected benefits of NEC is the ability to change how business is done as time passes. The effects of this can be examined in the analysis by exploring different combinations of the templates over the course of a campaign.

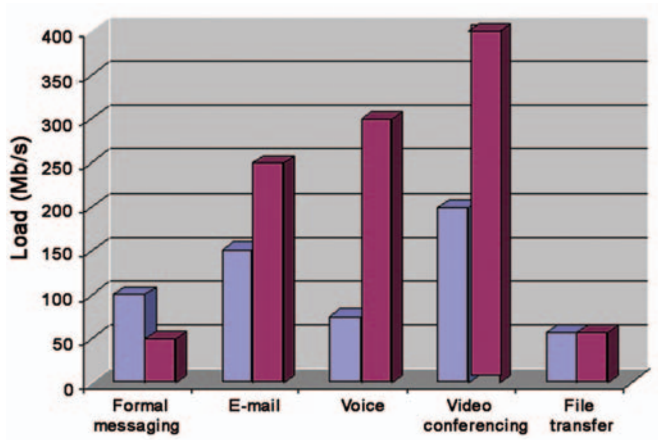


Fig 3. Comparison of the demand for information services from two different NEC concepts

3 COMET (COMmunication Evaluation Tool).

3 Test the demand against the capabilities of planned communications infrastructures

The next step tests the ability of defined communication structures to support the desired information exchanges. Slices of time (normally five hours to capture network latency issues) are chosen during which the information demand is highest. The ability of a network to handle the IERs from this period is then examined using COMPEAT[4]. This is a high-level resource-scheduling tool that is used to assess the performance of communication networks in a wide range of system configurations. COMPEAT attempts to send each IER occurring within the time slice from its source to its destination over the communications network specified for the given scenario. It determines the ability of the network to cope with the demanded information load, and it is also used to explore the impact of changes to assumptions. The model determines the percentage of traffic offered to the network that was successfully processed. To be considered successful, a message must be delivered within its predetermined timescale.

This approach can be used to explore the impact of NEC options on the performance of potential future communications infrastructures, and can help to identify potential changes to that infrastructure to support new ways of working. In addition, the effect of NEC options on the whole-life cost of planned communications can also be assessed, helping the decision-maker to judge the relative cost-effectiveness of different options.

4 Determine the effect on campaign-level measures of effectiveness

The final step is to quantify the impact of NEC options on campaign outcome through use of CLARION and COMAND high level models. This step can only be taken when the perceived benefits of the NEC option can be captured adequately in high-level campaign models. While some time-line issues may be captured directly (eg, delays in mission planning), this in general depends upon the existence of lower-level analysis and experimentation to determine and quantify the benefits at mission level.

[4] COMPEAT (COMmunication Performance Evaluation and Assessment Tool) has been developed and is used by Information Management Department, Dstl, and Communications Sector, QinetiQ.

CONCLUSIONS

NEC has much to offer to defence capability. It is important to ensure that it delivers feasible and cost-effective improvements. We have described a method that helps to inform decision makers on two issues: testing the impact of potential options (including those related to changes in the ways of doing business) on planned future communications infrastructures, and helping to identify the capabilities needed to support these NEC concepts. The method can also help to test the effect of these concepts on the outcome of campaigns. Plans are being developed to apply the method to emerging NEC concepts.

Policy and Capability Studies Department, Dstl, Cody Technology Park, Ively Road, Farnborough, Hants GU14 0LX
lcsharp@dstl.gov.uk

Quantifying the benefit of collaboration across an information network

James Moffat
Policy and Capability Studies Department, Dstl

Abstract
Network enabled capability can be assessed from many aspects: the two particular studies discussed here address, first, theatre ballistic missile defence, specifically, the best way of defending deployed troops in theatre against ballistic missile attack, and secondly, possible options for future headquarters structures. Methods for defending troops against ballistic missile attack are wide-ranging; the crucial factor in achieving disruption is time because the window of opportunity is narrow, while sure knowledge is a measure of the benefit of collaboration because it reduces uncertainty. Mathematical relationships are derived that enable information processing implications to be quantified to support a spreadsheet model. A headquarters' capability is determined by the quality of decisions. Methods of improving the representation of human decision-making in spreadsheet form are being developed. The model will be applied in the first instance to the concrete example of a logistics problem.

INTRODUCTION

The potential benefits of Network Enabled Capability (NEC) are being examined. In this paper, we discuss two studies: the first is concerned with Theatre Ballistic Missile Defence (TBMD), specifically, the best way of defending deployed troops in theatre against ballistic missile attack; the second examines possible options for future headquarters structures.

The pillars of a TBMD capability range from deterrence at one end, through counter-force options, to active and passive defence at the other. Here, we focus on the analysis that has been carried out in considering the place of counter-force in such a defensive mix. In particular, we look at the development of quantifiable methods to measure the overall benefit of sharing information across an information network to enhance the effectiveness of counter-force operations.

We are concerned here with assessing the position of a time-critical target (a ballistic missile launcher), and then vectoring an attack asset on to the target to destroy it. In this situation, time is of the essence. If we have a network of information elements sharing information to expedite such a process, the most straightforward way to capture this is to represent a network as a series of flows of information. Each of the nodes can then be considered as a processing element, which requires a certain time (or a distribution of times) to process the information and pass it forward through the network. Such an approach has been developed by Dstl. Building on work by the RAND Corporation for the US Navy, Information Entropy was used as the basis of a measure of the benefit obtained by a number of such nodes collaborating across an information network to increase the window of time during which time-sensitive targets can be prosecuted.

Information Entropy captures the uncertainty across the network; thus its inverse, which represents Network Knowledge, is a measure of the benefit of collaboration. A spreadsheet model (SIMCOM) has been produced that allows both the benefits and penalties (for example, information overload) of such NEC to be quantified. Thus, if the network nodes are considered simply in terms of their ability to process information in a timely way, the SIMCOM model can be used to explore the implications of various network assumptions on network collaboration. Later in the paper, we shall give some detail of the mathematical relationships that facilitate quantification.

The second study, on future headquarters structures, has considered a broad canvas of elements in the analysis, including interviews with senior military officers and the effects of concurrency in terms of the likely provision of such headquarters elements. As part of the current phase of studies, there was a need to develop a means of considering various decision-making elements of a future headquarters, and how they might link across an information network.

We have thus attempted to build a spreadsheet model of networked headquarters elements that takes into account not just the time to process information but the benefit of collaboration in terms of improved decision-making. Building on the previous work and ideas related to the SIMCOM model, we aim to produce a spreadsheet model that quantifies the improvement in decision-making arising from collaboration of information elements across an information network. Information Entropy is again the basis of quantifying improvement, and we explain why this is so later in the paper. In addition, we also wish to quantify the penalties of such collaboration, again building on previous ideas. Later on, we shall discuss how we can capture effects in a quantifiable way as part of joint work with the RAND Corporation. By bringing together two approaches, one that relates to our understanding of decision-making (the Rapid Planning process [1]) and the other relating to the benefits of information sharing based on Information Entropy [2, 3], we also meet most of the criteria for such a high-level representation listed in recent work by Fidock [4].

THE NETWORK AS AN INFORMATION PROCESSING SYSTEM

We consider here a command and control system put in place to aid the detection and prosecution of time-critical targets (ballistic missile launchers). We thus assume we have a network of Command and Control nodes, which are involved in coordinating this counterforce operation in the context of providing theatre ballistic missile defence to deployed UK forces. Each of these nodes has a number of information processing tasks to perform. If $\frac{1}{\lambda_i}$ is the mean time for node i to complete all of its tasks, we assume that this completion time is distributed exponentially (an exponential distribution is used to model the time between events or how long it takes to complete a task), so that if $f_i(t)$ is the probability of completing all tasks at node i by time t, then

$$f_i(t) = \lambda_i e^{-\lambda_i t}.$$

In general, there will be a number of parallel and sequential nodes in the network sustaining the counter-force operations. Let this total number be τ. In the simplest case, there is a critical path consisting of ρ nodes where ρ is a subset of τ, as shown below.

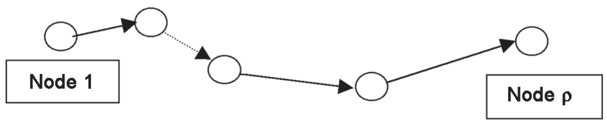


Fig 1. The critical path

We define the total latency of the path as the sum of the delays (latencies) at each of these nodes, plus the time, defined as t_m, required to move a terminal attack system (such as an aircraft) to the terminal attack area. In this sequential case, the total expected latency T is the sum of the expected latencies at each node on the critical path, plus the time t_m:

$$T = \sum_{i=1}^{\rho} \frac{1}{\lambda_i} + t_m$$

If there are sequential and parallel nodes on the critical path, these can be dealt with in the way shown by the example below.

In this example, $T = \max(\frac{1}{\lambda_1}, \frac{1}{\lambda_2}) + \frac{1}{\lambda_3} + \frac{1}{\lambda_4} + t_m$

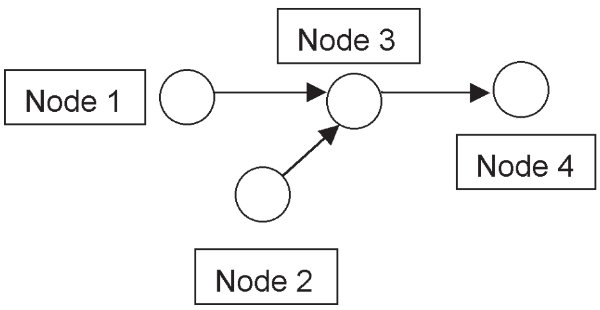


Fig 2. Parallel nodes on the critical path

Returning now to the case of a serial set of nodes, for each such node i on the critical path, define the indegree d_i to be the number of network edges having i as a terminal link. For each node j in the network, we assume [2] the amount of knowledge available at node j concerning its ability to process the information and provide quality collaboration to be a function of the uncertainty in the distribution of information processing time $f_j(t)$ at node j. Thus the more we know about node j processes, the better the quality of collaboration with node j.

Let $H_j(t)$ be the Shannon entropy of the function $f_j(t)$. Then $H_j(t)$ is a measure of this uncertainty defined in terms of lack of knowledge. By definition of the Shannon entropy, we have:

$$H_j(t) = -\int_0^{\infty} \log(\lambda_j e^{-\lambda_j t}) \lambda_j e^{-\lambda_j t} dt$$

Since the differential of $(xe^x - e^x)$ is xe^x ,

it follows that $H_j(t) = \log(\frac{e}{\lambda_j})$

If we consider distributions of the processing time t, then clearly t is restricted to positive values. It then follows that the exponential distribution we have assumed is the one giving maximum entropy (Shannon [5]). Our assumption for information processing times is thus conservative.

If $\lambda_j$min corresponds to a minimum rate of task completions at node j, then $\frac{1}{\lambda_j \min}$ corresponds to a maximum expected time to complete all tasks at node j. To provide a normalized value of the knowledge $K_j(t)$ available at node j in terms of the Shannon entropy, reference [2] defines this as:

$$\begin{aligned} K_j(t) &= \log\left(\frac{e}{\lambda_j \min}\right) - \log\left(\frac{e}{\lambda_j}\right) \\ &= \log\left(\frac{\lambda_j}{\lambda_j \min}\right) \text{ where } \lambda_j \min \le \lambda_j \le e\lambda_j \min \\ &= 0 \text{ if } \lambda_j < \lambda_j \min \\ &= 1 \text{ if } \lambda_j > e\lambda_j \min \end{aligned}$$

Suppose now that node i is on the critical path, and node j is another network node connected to node i. Let c_{ij} represent the quality of collaboration obtained by including node j. If this is high, we assume $K_j(t)$ will be close to 1. The effective latency at node i is then assumed to be reduced by the factor $(1-K_j(t))^{\omega_j}$ owing to the effect of this high quality of collaboration. The factor ω_j is assumed to be 1 if j is one of the nodes directly involved in the counter-force operation (but not on the critical path). It is assumed to be 0.5 if node j is one of the other network nodes.

We are assuming here that the ability to use the time more wisely through collaboration (to fill in missing parts of the operational picture that are available from other nodes, etc) has an impact that can be expressed equivalently in terms of latency reduction. The use of such time more wisely implies a good knowledge of expected times to complete tasks that can provide such information. Exploiting Shannon entropy as the basis for such a Knowledge function was first developed as part of the UK Airborne Stand off Radar (ASTOR) force mix analysis in the context of ASTOR as a wide area sensor available to the Joint or Corps commander. The gaming-based experiments carried out [6] indicated that Knowledge correlates directly with higher-level measures of force effectiveness (such as reduction in own force casualties) for warfighting scenarios. We are assuming a similar process is at work here –reduced entropy (ie, reduced uncertainty) leads to improved Knowledge, and hence to improved ability to carry out the task.

The total (equivalent) reduction in latency at node i because of collaboration with the network nodes connected to node i is then given by:

$$\begin{aligned} c_i &= \prod_{j=1}^{d_i} c_{ij} \\ &= \prod_{j=1}^{d_i} (1 - K_j(t))^{\omega_j} \end{aligned}$$

Thus the total effective latency along the critical path, accounting for the positive effects of collaboration, is given by:

$$\begin{aligned} T_c &= \sum_{i=1}^{\rho} \frac{c_i}{\lambda_i} + t_m \\ &= \{\sum_{i=1}^{\rho} \frac{1}{\lambda_i} \prod_{j=1}^{d_i} (1 - K_j(t))^{\omega_j}\} + t_m \end{aligned}$$

The penalty of collaboration

Reference [2] now includes a 'complexity penalty' to account for the fact that including additional network connectivity leads to information overload effects. This is the negative effect of collaboration. It leads to an increase in effective latency on the critical path. Following [2], we define C to be the total number of network connections accessed by nodes on the critical path. For each node i on the critical path, this is the indegree d_i. Thus $C = \sum_{i=1}^{\rho} d_i$. The value of C is then a measure of the complexity of the network. We assume that the complexity effect as a function of C follows a non-linear 'S' shaped curve as shown in figure 3.

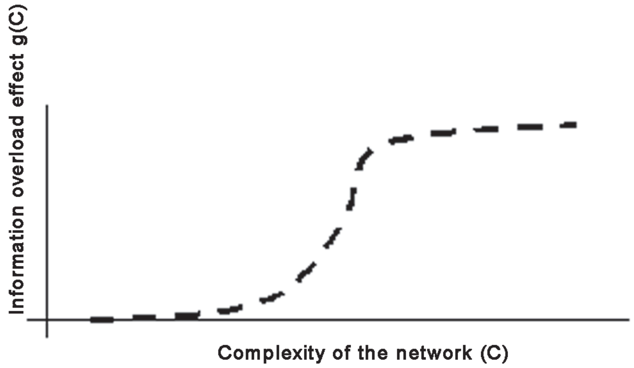


Fig 3. The logistics S-shaped curve

The relationship used to describe this effect is a logistics equation:

$$g(C) = \frac{e^{a+bC}}{1 + e^{a+bC}}$$

The penalty for information overload is then defined as

$$\frac{1}{1 - g(C)}$$

The total effective latency, taking account of both the positive and negative effects of C2 network collaboration, is then:

$$T_{c,C} = \frac{T_c - t_m}{1 - g(C)} + t_m$$

In terms of the SIMCOM modelling approach, we define the distribution of response time, given a detection. Given a target detection at time t, this network-enabled approach allows us to compute the distribution of response time $R_d(t)$ as a function of the network assumptions (eg, platform centric, network centric, futuristic network centric to use the RAND categories [2]).

THE NETWORK AS A DECISION-MAKING SYSTEM

In considering the networked structure of future headquarters from a capability perspective, it is not enough in itself just to consider them as sets of nodes that process information, since time-critical targeting is but one aspect of a network. Going beyond this, we would wish to understand how different such information sharing options could improve the quality of decisions made by commanders. A collaborative research programme with RAND has led to a fuller understanding of the theory of how to create such a representation. This exploits Dstl work on the development of improved representation of human decision-making and related aspects of command and control in fast-running agent-based simulation models such as WISE, COMAND and SIMBAT [1]. It also exploits work by RAND sponsored by the US Navy [2, 3] and the Swedish Department of Defence. A joint RAND and Dstl report will appear shortly that describes this theory in detail.

In parallel, a first version of a spreadsheet model is being produced. The aim of this first version is to represent the theory developed in the joint RAND/Dstl report, and to apply it to a particular example. The example is based on the command and control of logistics and, in consultation with General Sir Rupert Smith, we have focused first on fuel supply. Three possible options have been worked up in detail, which we call Demand led, Supply led and Directed. The Directed form (a term and concept developed by General Smith on the basis of Gulf war experience) represents a balance between the supply led and demand led concepts, and links to the fireplan and synchronization matrix developed and evolved as the battle goes forward. The theory developed and the structure of the spreadsheet allow all of these options to be explored.

The theory is deep (much deeper than that used in the SIMCOM model), and we are still working out how exactly to capture it in the spreadsheet. We hope to have a first version available shortly, capable of coping with the logistics example outlined above. This will then be further developed in collaboration with RAND. A summary of the theory that we have now developed is given next.

A SUMMARY OF THE THEORY NOW DEVELOPED

We are dealing with a number of decision-making nodes, which make decisions on the basis of information either available to them locally or through sharing of information across an information network. These nodes thus represent key points at which significant decisions are made. They are supported by other nodes, which represent information sources such as sensors or fusion centres. Figure 4 shows a network of decision-making nodes, with information coming in either directly or through the network.

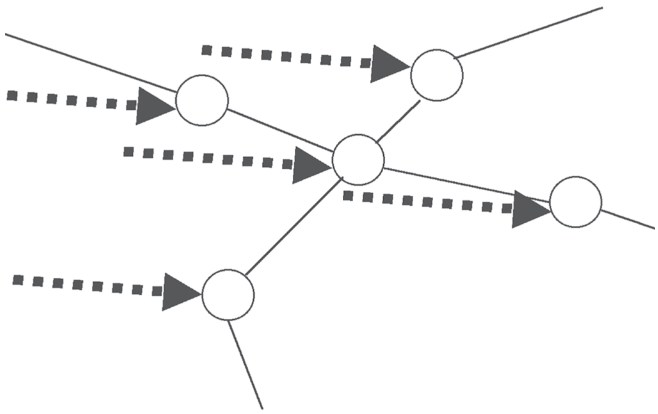


Fig 4. A network of decision-making nodes

We take as our reference model that developed by Alberts *et al* in their description of information age warfare [7]. As, shown in figure 5, we are looking at the information available to one or several of these decision-making nodes, and then transforming that into a quantified measure of Knowledge across the network. This represents the benefit to be derived from collaboration as measured at the cognitive level. We also look at the costs and penalties of such a collaboration.

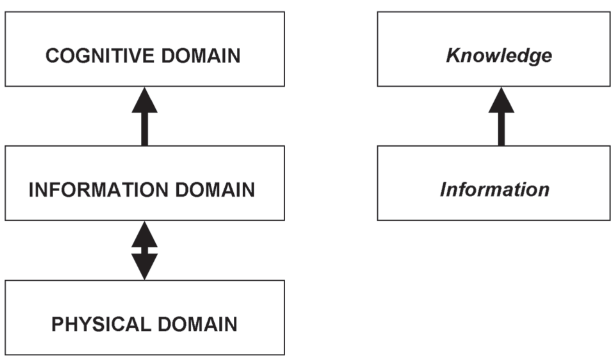


Fig 5. Reference model

First let us look at a single node. As remarked earlier, we represent the decision-making process at the node by using the Rapid Planning process. The gist of this approach is shown in figure 6. The general structure shown appears to capture well the decision-making process of commanders in fast and rapidly changing circumstances. We assume that the situation awareness of the commander (and hence of the decision-making node that represents him) is formed by a small number of key variables or attributes. We show two in the picture at figure 6. The commander aims to understand where he is currently in the 'conceptual space' spanned by these attributes. This is shown by the ellipse in figure 6 corresponding to a best estimate and an area of uncertainty. The commander then tries to match this appreciation to one of a number of fixed patterns in the space in order to understand which course of action to carry out based on this local perception. At the basic level, these patterns would correspond to an area within which he is 'OK' (ie, a 'comfort zone' within which he is happy with his current perception of the key parameters, and how these relate to his ability to carry out his mission), and the complement of this area where he is 'not OK'. This approach was developed from psychological research based on naturalistic decision-making [1] and most recently endorsed by General Smith in discussion of his command of the UK land forces during the Gulf war.

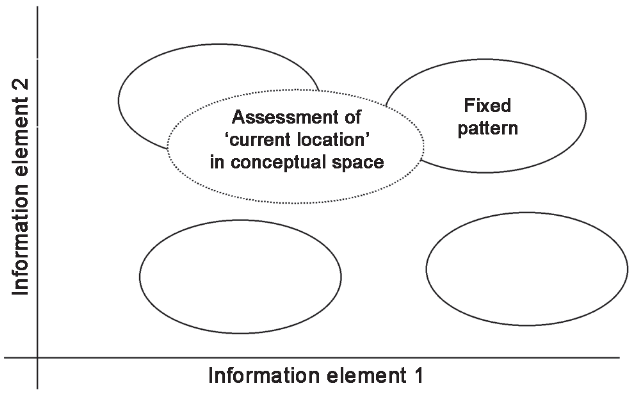


Fig 6. The rapid planning process

Consider now a simple example of collaboration between two such decision-making nodes. We assume that these correspond to two brigades, each with a demand for fuel from the logistics supply system. In the first case, we assume that the two brigades do not collaborate, and that fuel is supplied to them on a 'top-down' supply basis, informed by the general plan of operations, modified only by changes to the plan as we move through the phase lines of the operation. In this case, the local assessment of demand at Brigade 1 will have a mean and a variance. Similarly, the local estimation of demand at Brigade 2 will have a mean and a variance. Figure 7 shows the means at the origin, and the variances give rise to an area that corresponds to the area of uncertainty about these mean values.

Since we have two means and two variances, we have a 2-dimensional distribution of demand (rather like the scatter of points about the bullseye of a dartboard) and the dotted ellipse in figure 7 is an assessment of the scatter or uncertainty in the assessment of this demand. Because there is no information sharing between the brigades, there is no interaction, ie, *no correlation* between the estimates for the two brigades. This means that the ellipse of uncertainty is not skewed, and sits as shown in the figure. Clearly, there are two ways to reduce the area of uncertainty: we can either shrink the size of the dotted ellipse (corresponding to reducing the variance of each of the estimates) or we can squash the ellipse into the other shape, shown in figure 7 by the bold line. Shrinking the dotted ellipse is achieved by reducing the variance estimates for each of the brigades. Squashing the ellipse is achieved by building up a correlation between the variables (ie, an understanding of how the variables relate to one another). In either case, this can only be achieved by sharing information.

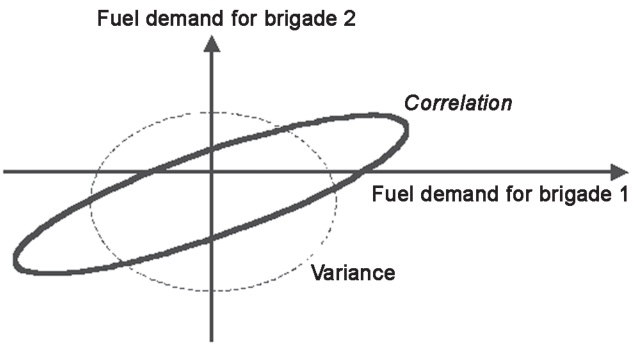


Fig 7. Variance and correlation

In the most straightforward case, we assume that the demand for fuel at each brigade can be modelled as a normal distribution[1]. If we then track the demand for fuel for both brigades, we shall have a distribution of two variables (the demand for fuel at each brigade), which is known as a Bivariate Normal distribution. The ellipses in figure 7 then correspond to lines of equal probability from this joint distribution. As we have seen, a good measure of overall uncertainty is the area within such an ellipse. In turn, this can be captured by the entropy of the bivariate normal distribution. In more detail, the covariance matrix of the bivariate normal distribution captures the variance of demand at each brigade, and also the correlation of demand between the brigades. From the definition of Information Entropy, (see for example Shannon [5]) it can be shown that the entropy of the bivariate normal distribution of demand is given by the logarithm of the determinant of this covariance matrix. This is essentially a measure of the area within the ellipses shown in figure 7.

[1] Note: The same argument applies if we assume a lognormal distribution. In this case, we consider the logarithm of the time series of demand, which is then normally distributed. The lognormal distribution has the attribute of being defined over the range zero to infinity.

Thus reducing entropy leads to reduced uncertainty about where we are in our conceptual space (here bounded by the two information elements of fuel demand at each of brigades 1 and 2). The inverse of entropy (which is a measure of knowledge) is then the basis for a measure of the benefit to be obtained from information sharing to reduce the area of such ellipses.

This whole argument can be (and has been) extended mathematically to a space of n-dimensions rather than two. This corresponds to a number of nodes, and a number of key information attributes.

In summary, we have shown that the benefit of sharing information is captured through looking at the joint distribution of the key elements of information across the collaborating nodes, quantifying the Information Entropy of that distribution, and comparing the result with the entropy corresponding to the nodes acting separately (ie, not collaborating). We have also shown that a key aspect of this is the build up of correlation between these key elements of information (ie, how one variable relates to another), which sits well with our common sense understanding of an increase in knowledge of a situation.

The next question is –what happens if the key elements of information (fuel demand of the brigades in the example above) are not normally distributed? RAND have researched this issue in their work for the US Navy. The situation is most easy to cope with if there is still a known joint distribution across the key elements of information. In this case, the theory of 'relative entropy' can be used to assess the 'mutual information' added by the understanding of how one information element relates to another. Where there is no joint distribution, more empirical methods have to be used to assess the interaction between variables, and RAND have considered a number of these in their work [3].

Finally, assuming that we can make a basic assessment of the benefit of collaboration among a group of nodes in terms of information entropy, we now have to turn this into a fully quantified measurement of both the benefits and the penalties of collaboration. We have put forward an approach to this that proceeds by a number of steps. First, we take our measure of benefit based on entropy (recall that this relates to the variance of estimates) and turn it into a measure of the 'precision' of our understanding. This is combined with a measure of the 'accuracy' of our understanding (roughly; where our mean value is relative to ground truth) to produce a combined measure of benefit. (This process involves curve fitting that will require calibration by experiment.) This is then combined with a measure of the 'completeness' of the information to produce an overall metric of the benefits of collaboration arising from information sharing and the interaction between the key information elements.

Figure 8 indicates how the 'precision' and 'accuracy' measures are combined into a single metric. The curve fitted to each variable is a Beta distribution [3]. This represents a hypothesized relationship that will require calibration by experiment. As part of future work by RAND with the US Navy, experiments are planned to do just this.

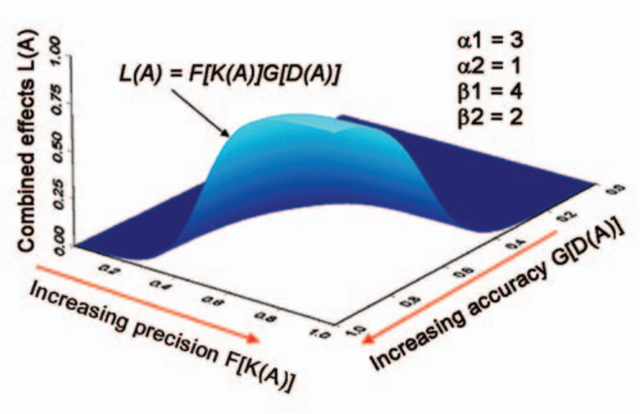


Fig 8. Combining 'precision' knowledge and 'accuracy' knowledge

Completeness

At any decision node i, we define the complete data set up to the critical decision point t as the set $\mathbf{x}_{i,t} = \left[x_{i,t,1}, x_{i,t,2}, \cdots, x_{i,t,N} \right]$. The set consists of N elements of critical information, but in fact only n $\leq$ N out of N might be available at time t; then the value of completeness at node i is defined as $X_{i,t}(n) = \left[\frac{n}{N} \right]^{\xi}$, where ξ is a 'shaping' factor [3]. For values of $\xi < 1$, the curve is concave downwards, for $\xi > 1$ it is concave up and for $\xi = 1$ it is a straight line. The selection of the appropriate value depends on the consequences associated with being forced to take a decision with incomplete information. This measure of *completeness* can be enhanced to include the effect of *freshness* of information, and to include the effect of the network 'reach' required to deliver such information [8].

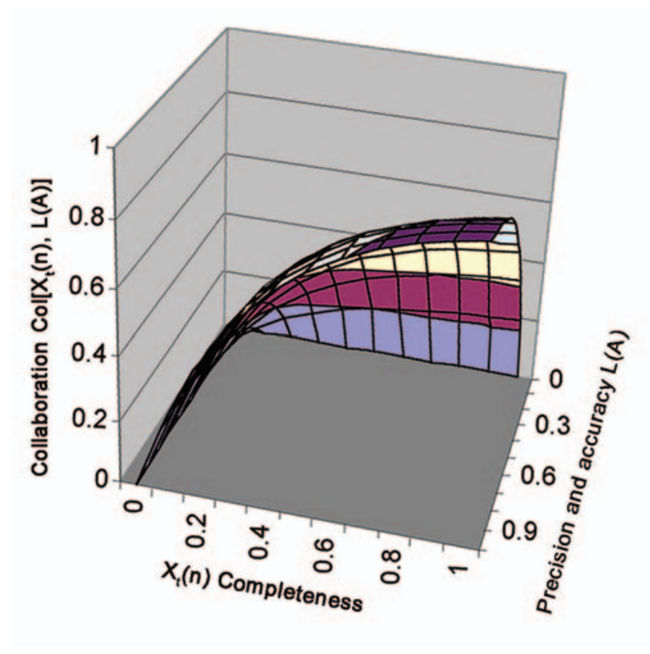


Fig 9. The benefit of collaboration as a function of completeness, 'precision' knowledge and 'accuracy' knowledge

Folding completeness into the metric gives an overall relationship between the benefit of collaboration on the one hand and the influence of completeness, 'accuracy' knowledge and 'precision' knowledge on the other, as shown in figure 9. This again represents a hypothesized relationship that will require calibration by experiment.

This metric on its own would lead to the assessment that larger and larger collaboration across a network is of continuing benefit. This is clearly not always the case. We thus need to temper the assessment by measures of the cost of dealing with inconsistent evidence, information overload, etc. These various factors have been quantified (again as curves that will require experimental validation [3]). The combination of the benefits and penalties of collaboration we call the 'Network Plecticity' (a term taken from complexity theory [9]). It gives an overall metric for quantifying the implications of collaboration between decision-making nodes across an information network.

CONCLUSIONS

By considering a network of information sharing and decision-making elements first as a system of information processing elements, we have shown that it is possible to quantify the benefits and penalties associated with information sharing across such a network. This work has already been applied to produce valuable insights as part of a study of Theatre Ballistic Missile Defence. Building on this approach, and in collaboration with RAND, we have extended the theory to examine the likely impact of such information sharing on the quality of decision-making. A high-level spreadsheet model based on this theory is being developed and will be applied in the first instance to information sharing across a logistics network.

Acknowledgements

The author acknowledges the contribution of Dr Lorraine Dodd, QinetiQ, and Dr Walt Perry, RAND Corporation, to this work.

References

1 Moffat J. *Command and control in the information age; representing its impact*. The Stationery Office, London (2002).

2 Perry W L *et al*. *Measures of effectiveness for the information age navy; the effects of network-centric operations on combat outcomes.* RAND MR-1449-Navy, RAND, USA (2001).

3 Perry W L *et al. Advanced metrics for network-centric naval operations.* RAND Report 2834-Navy, RAND, USA (2002).

4 Fidock J. *Building representations of organisational behaviour in models of military headquarters*. Dstl Unpublished Report (September 2002).

5 Shannon C E. *A mathematical theory of communication*. The Bell System Technical Journal **27**, 379 and 623 (October 1948).

6 Perry W L and Moffat J. *Measuring the effects of knowledge in military campaigns.* J Operational Research Soc. **48** No. 10 (1997).

7 Alberts D S and Garstka J J *et al*. *Understanding information age warfare*. DoD Command and Control Research Program, Department of Defense, USA (2001).

8 Perry W L and Moffat J. *Information sharing among military headquarters: the impact on decision making.* Joint RAND/Dstl Report. In draft.

9 Gell-Mann M. *Let's call it plectics.* Complexity **1** No 5 (1995).

Dstl, Cody Technology Park, Farnborough, Hants GU14 0LX
JMOFFAT@mail.dstl.gov.uk

The coalition agents experiment: network-enabled coalition operations

David Allsopp, Patrick Beautement and Michael Kirton
Distributed Technology Group, QinetiQ Ltd

Jeffrey M Bradshaw and Niranjan Suri
Institute for Human and Machine Cognition, University of West Florida

Austin Tate
Artificial Intelligence Applications Institute, University of Edinburgh

Mark Burstein
BBN Technologies

Abstract
Multinational coalitions are increasingly important in military operations. But coalitions today suffer from heterogeneous command systems, labour-intensive information collection and coordination, and different and incompatible ways of representing information. The purpose of Network Enabled Capability (NEC) is to enhance military capability by exploiting information better. The Coalition Agents Experiment (CoAX) was an international collaborative research effort to examine how the emerging technologies of software agents and the semantic web could help to construct coherent command support systems for coalition operations. Technology demonstrations based on a realistic coalition scenario showed how agents and associated technologies facilitated run-time interoperability across the coalition, responded well to unexpected battlespace events, and aided the selective sharing of information between coalition partners. We describe the CoAX experiments, the approaches and technologies used, and highlight how they support the NEC concept. CoAX produced a prototype 'Coalition agents starter pack" that could be developed further to support coalition warfare.

1 INTRODUCTION

Military context

Success in military operations calls for high-tempo, coherent, decisive actions (faster than an opponent can react) resulting in decision dominance through the use of command agility – the flexibility and adaptability to grasp fleeting opportunities. To achieve this, the commander must issue clear intent and then delegate the control authority to subordinates, allowing them the scope to exercise initiative. It also means being innovative, creative and unpredictable, to increase confusion in the mind of an opponent. This process is command led, which means that human decision-making is primary and the role of technology secondary. Shared understanding and information superiority are key enablers in this process and are fundamental to initiatives such as NEC. Indeed, the aim of NEC is to enhance military capability through the better exploitation of information.

The current reality of coalition operations is often a picture of data overload and information starvation, labour-intensive collection and coordination, individual stovepipe systems, incompatible formats, scattered snapshots of the battlespace and a horrendous technical integration task. This paper aims to show that the agent-based computing paradigm offers a promising new approach to dealing with such issues by embracing the open, heterogeneous, diverse and dispersed nature of the coalition environment.

Technical approach

Agents are software components that are goal-oriented, active and social [1]. They operate in the digital world and can work on behalf of people to provide the information and services users need [2-4]. The premise of our research is that software agents and associated technologies (discussed further in section 3) provide a powerful conceptual basis for developing large-scale, open, distributed systems for the battlespace in which warfighters and computer systems must work and share information together in a seamless and flexible manner. This will enable warfighters to acquire, visualize and manipulate diverse and dynamic information –however they wish and whenever they need it –putting them in control.

The focus of our research was on creating and demonstrating an agent-enabled infrastructure that would support multinational coalition operations. In addition to the problems of integrating single-service and joint capabilities into a coherent force, the nature of coalition operations implies some need to configure incompatible or foreign systems rapidly into a cohesive whole. Many such problems can only be solved by organizational changes and by aligning doctrine, concepts of operations and procedures. Coalition operations trigger the need for a rapid on-the-fly response and cannot be predicated on using pre-existing coordinated systems –hence the need for a flexible approach that allows capabilities to be assembled at 'run time'. However, in addressing this requirement for interoperability, it is also crucial to tackle issues of security of data, control over semi-trusted software from other coalition partners, and robustness of the resulting system. These were all addressed in our work. Furthermore, throughout this paper, we shall highlight where our research directly supports the following NEC core themes [5]:

- full information availability –enabling a user to search, manipulate and exchange information of different classifications captured by, or available in, all sources internal and external to the battlespace

- shared awareness –providing a shared understanding and interpretation of a situation, the intentions of friendly forces, and potential courses of action amongst all elements in the battlespace

- flexible working –enabling assets to reconfigure rapidly to meet changing mission needs, allowing them to work together with minimum disruption and confusion

- agile mission groups –enabling the dynamic creation and configuration of mission groups that share awareness and that coordinate and employ a wide range of systems for a specific mission

- synchronized effects – achieving overwhelming effects within and between mission groups by coordinating the most appropriate assets available in the battlespace through dynamic distributed planning and execution

- effects based planning –taking an approach to planning that focuses on the use of military and non-military effects against an enemy, and which is integrated with other planning processes in the battlespace

- resilient information infrastructure –ensuring information resources can be managed and that secure access is provided with the flexibility to meet the needs of agile mission groups

- fully networked support –allowing the ready use of non-frontline government bodies, industry, academia and public service capabilities to support operations.

The Coalition Agents Experiment (CoAX)
This international collaborative research programme ran from February 2000 to October 2002 [6]. It involved twenty-six formal partners from the UK, the US and Australia, with support from, among others, TTCP [7] and Defence Research and Development Canada. The CoAX web site maintains an up-to-date listing of participants [8]. QinetiQ researchers were members of the project 'Software Agents in Command Information Systems', which ran from April 1999 to December 2002 and was funded from MoD's Beacon initiative and the CISP (Communications Information and Signal Processing) technology domain of MoD's research programme. The US Defense Advanced Research Projects Agency (DARPA) supported the participants from the US, the University of Edinburgh and QinetiQ through the Control of Agent-Based Systems Programme (CoABS), a multi-million dollar effort that ran from 1997 to 2002 [9]. Australian researchers came from the Defence Science and Technology Organisation in Edinburgh, South Australia.

CoAX was a CoABS technology integration experiment led by a small team of principal investigators from QinetiQ, the Artificial Intelligence Applications Institute (AIAI) at the University of Edinburgh, the Institute for Human and Machine Cognition (IHMC) at the University of West Florida, and BBN Technologies. A series of CoAX demonstrations that showed increasing functionality was carried out between 2000 and 2002 –referred to as CoAX Binni 2000, CoAX Binni 2001 and CoAX Binni 2002. The final demonstration was held over two days in October 2002 at the US Naval Warfare Development Command, Rhode Island, before an invited audience of over a hundred senior officials from the US DoD, US military, US government agencies and UK MoD. This paper focuses on the CoAX Binni 2002 demonstration, though we briefly describe the 2000 and 2001 demonstrations to provide context.

CoAX Aims
The overall goal of CoAX was to show that an agent-enabled infrastructure could significantly aid the construction of a coalition 'command support system' and improve its effectiveness. More specifically, the operational and technical objectives of CoAX were to show how:

a) flexible, timely interaction between different types of potentially incompatible systems and information 'objects' could be effectively mediated by agents, leading to agile command and control, and improved interoperability

b) ease of composition, dynamic reconfiguration and proactive coordination of coalition entities lead to adaptive responses to unexpected events at 'run-time', providing robustness in the face of uncertainty

c) loosely-coupled agent architectures, where behaviours and information are 'exposed' to the community, are more efficient and effective than monolithic programs

d) agent policies and domain management help to facilitate:

   - selective sharing of information between coalition partners, leading to coherent operations

   - control of appropriate agent behaviour, leading to an assured and secure agent computing environment.

2 COALITION SCENARIO AND COMMAND STRUCTURE

Scenario
To create a suitably realistic scenario for the demonstrations, the CoAX team adapted and expanded the fictional Binni scenario [10-11] developed for TTCP [7]. It is set in 2012 on what is currently the Sudanese Plain (figure 1). Global

warming has affected agriculture and altered the world's political balance; a previously uninhabited land has become arable and has received considerable foreign investment. It is now called the 'Golden Bowl of Africa."

Fig 1. Binni and adjacent countries

A conflict has developed between two countries in the area: Gao to the north and Agadez to the south. Gao has expansionist aspirations but is only moderately developed, possessing old equipment and a mostly agrarian society. Agadez is a relatively well-developed fundamentalist country. Gao has managed to annex an area of land, name it Binni, and establish its own puppet government, which has then come under fierce attack from Agadez. Gao, voicing concerns about weapons of mass destruction, has enlisted UN support to stabilize the region. Arabello is a country on the eastern edge of the Red Sea that becomes involved and eventually provides anti-submarine warfare (ASW) capabilities to the coalition.

Coalition command structure

As the coalition forms, it needs to configure a variety of incompatible stovepiped systems rapidly into a cohesive whole within an open, heterogeneous, dispersed environment. The complexity of this environment is exemplified through the Binni coalition command structure shown in figure 2.

This representative and realistic coalition command structure involves the UN, governments, other government departments (such as the Foreign Office), non-government organizations (such as Oxfam), representatives of all the coalition countries (with their own 'ghosted' command structures, shown as dotted lines), and the coalition headquarters and subordinate fighting forces. The participants would normally agree to the coalition structure when it is formed; no specific country owns any part of the formal command chain, and levels of command overlap, with no rigidly defined boundaries. Dashed lines show an advisory or negotiating role.

From the human perspective, we identified four types of domains (which overlap and are not mutually exclusive) in the Binni coalition:

- organizational, such as the coalition force headquarters
- country, with each national command chain a separate, self-contained domain
- functional, where entities collaborate on common tasks such as meteorology or intelligence
- individual human domains of responsibility, where commanders have responsibility for their own headquarters and all subordinate ones.

3 ENABLING TECHNOLOGIES

We researched and developed a number of emerging technologies, centred around the agent computing model, to facilitate the rapid and seamless sharing of data and information in distributed enterprises. Figure 3 shows how the technologies are linked. Their descriptions follow.

Software agents

Agents can be viewed as semi-autonomous entities that help people to cope with the complexities of working collaboratively in a dispersed information environment [2]. A community of agents works as a set of distributed, asynchronous processes,

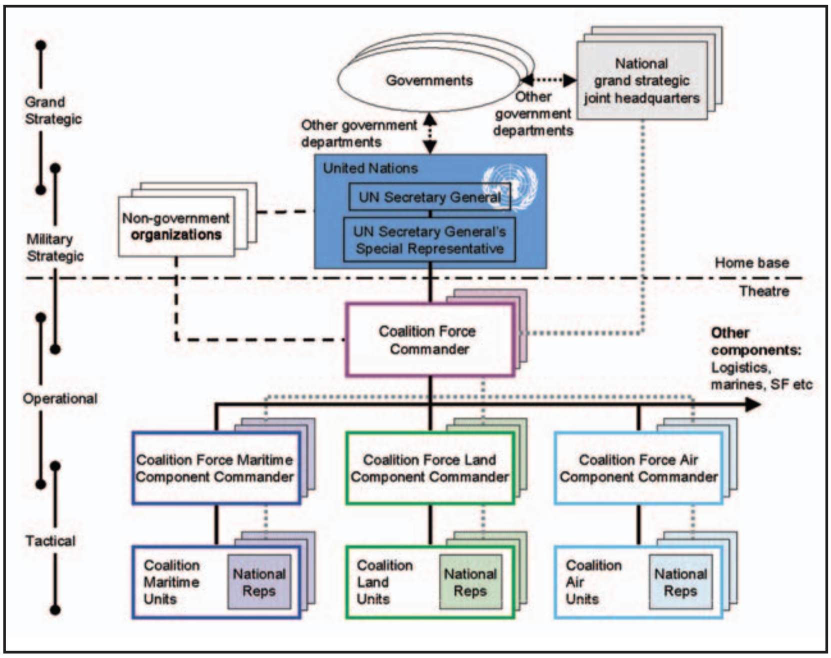


Fig 2. This representative coalition structure shows the chain of command down from the United Nations. The solid black lines show the legal lines of authority (the command chain) and accountability. Dashed lines show an advisory or negotiating role and dotted lines the 'ghosted' command chains of the participating nations. The approximate command levels at which the various entities operate are on the left.

Human-cyberspace interface: interface agents, augmented cognition, ubiquitous computing
Semantic web: facilitates common understanding of terms, relations and services across communities
Agent-based computing: provides glue to link and interoperate disparate systems and applications; provides services that facilitate interoperability
Grid infrastructure: generic middleware for building distributed applications and creating virtual organizations; security, dependability, data exchange

Fig 3. Emerging technologies for information sharing in distributed enterprises. The name of each layer is followed by a brief description of its properties.

communicating and sharing information by passing messages in a digital infrastructure. Essentially, agents communicate with users and among themselves to find, format, filter and share information. They work with users to make this information available whenever and wherever they need it, and can be organized to support individuals, military commands and virtual function teams [4]. Agents can also suggest courses of action proactively, monitor mission progress, and recommend plan adjustments as circumstances unfold. Moreover, the agent paradigm provides the modularity and abstraction required for building large, distributed and complex software systems [12].

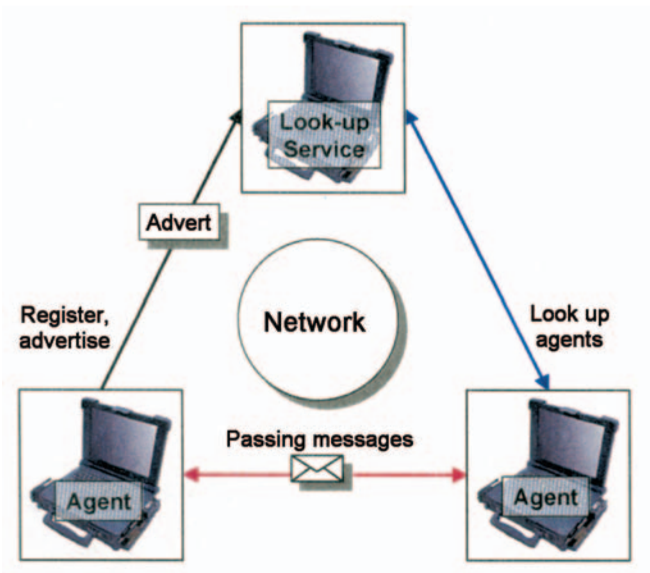


Fig 4. Representation of a network of computers showing multiple inter-operating software agents. Grid software provides look-up services that are used to register and advertise agents and communication services for passing messages between agents. Agents and look-up services can be distributed flexibly across the network, with multiple agents per machine if required.

The CoABS grid

Agents and systems that are to be integrated in a network-enabled environment require an infrastructure for discovering other agents and passing messages between agents. The CoABS grid [9] provided this capability in the series of CoAX experiments (figure 4). The CoABS grid middleware included an interface to register agents, advertise their capabilities, discover agents based on their capabilities, and send messages between agents. It also provided a logging service for both message traffic and other information, a security service to provide authentication, encryption and secure communication, and event notification when agents register, de-register, or change their advertised attributes.

The CoABS grid is based on the Java language and Jini networking technology from Sun Microsystems, making use of two important components of Jini:

- *look-up services*, which are used to register and discover agents and other services. Multiple look-up services can be run for robustness and scalability

- *entries*, which are placed in the look-up services by agents to advertise their capabilities.

Operators or even agents themselves can add or remove agents on the CoABS grid or update their advertisements without network reconfiguration. Agents that fail are automatically purged from the look-up services.

Agent domains and policies

The increased intelligence that software agents provide is both a boon and a danger. Because they operate independently without constant human supervision, agents can perform tasks that would be impracticable or impossible using traditional software applications. However, this autonomy, if unchecked, could also severely impair military operations if defective or malicious agents were to arise.

In CoAX, the Knowledgeable Agent-Oriented System (KAoS) provided services to assure that agents from different developers and running on diverse platforms always operated within the bounds of established policies, and were continually responsive to human control to permit safe deployment in operational settings [13-15]. KAoS services and tools permitted policy management within the specific contexts established by complex military organizational structures.

KAoS policy and domain management services organized agents into logical groups corresponding to organizational structures, administrative groups and task-oriented teams. Within CoAX, these domains mirrored the human domains described in section 2, allowing for complex hierarchical and overlapping structures. An agent domain consisted of a domain manager component and any agents registered to it. The domain manager managed agent registration and served as a point of administration for the specification, analysis and conflict resolution, distribution and enforcement of policies, represented in DARPA Agent Mark-up Language ontologies (see below). Figure 5 shows a typical domain configuration built on the CoABS grid and domain management services of KAoS.

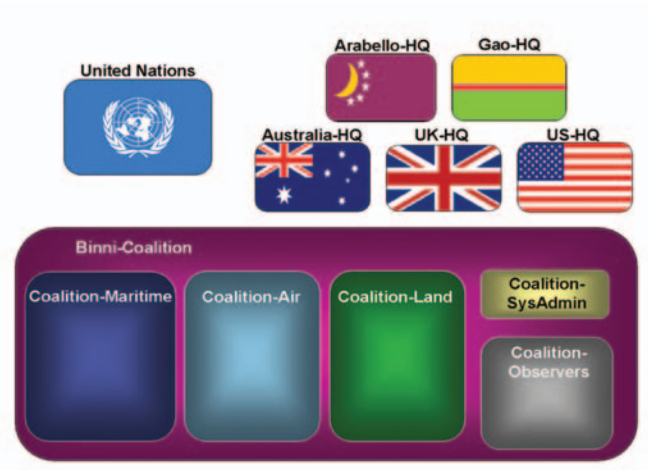


Fig 5. Domain structure used in the CoAX Binni 2002 demonstration. Rounded rectangles indicate domains; each domain would contain a variety of agents whose activities would be governed by a domain manager and matchmaker agent (omitted for clarity). Domain nesting indicates a hierarchy of responsibility and control.

Nomads, which consists of Aroma, an enhanced Java-compatible virtual machine, with its Oasis agent-execution environment, was used in conjunction with KAoS to enforce fine-grained resource control, and information filtering and transformation policies.

Semantic web

Currently, web pages are geared towards visual presentation of information for humans with no support for machine understanding, severely limiting the automated processing of the huge volumes of information on the web. In this context, the semantic web is a vision: the idea is to have data on the web defined and linked such that it can be used by machines not just for display purposes but for automation, integration, inference and reuse of data across various applications [16,17]. Clearly, to turn these ambitions into reality requires the development of new technologies, tools and methodologies. The semantic web model uses Uniform Resource Identifiers (URIs) to identify resources (electronic images, documents, services; web page addresses such as http://www.QinetiQ.com are a type of URI). The Extensible Mark-up Language (XML) is a meta-language that provides a flexible, extensible common text format for data exchange. Schemas and ontologies provide a means of describing the meaning of terms in a domain. In the semantic web, these are based on, for example, the Resource Description Framework and the DARPA Agent Mark-up Language (DAML) [18].

In the CoAX demonstrations, XML was one of the languages used for inter-agent messaging, and DAML was used to encode and reason about domain entities, domain policies and agent message contents. Semantic web ontology-based tools, such as the Decision Desktop (section 4, figure 10), were used for coalition-wide information gathering and visualization.

4 DEMONSTRATION STORY-BOARDS AND TECHNOLOGIES

The CoAX demonstrations were built around story-boards that described a set of events that were realistic in military terms. These are described next.

CoAX Binni 2000 demonstration: information gathering phase

The events of the CoAX Binni 2000 demonstration focused on the initial planning phase of conflict [6]. A number of options to separate the opposing forces and restore peace in the region, including the deployment of a large ground-observation and peace-enforcement force, had been rejected and a 'Firestorm' mission was chosen. The aim was to clear land and keep belligerent forces apart to facilitate simpler remote and ground observations with less risk to the coalition peacekeepers. The demonstration started by showing how the coalition used agents to gather initial information from among the partners. This provided coalition-wide shared awareness. During the course of events, it became clear that Gao was feeding misinformation, and special system administration steps were taken to monitor the information passed to and from Gao within the coalition (figure 6). Later, Gao became belligerent and launched a denial-of-service attack against the coalition's C4I infrastructure. This was automatically detected and thwarted using the advanced KAoS policy administration capabilities available to the coalition, coupled with fine-grained resource control available in Nomads [14,15].

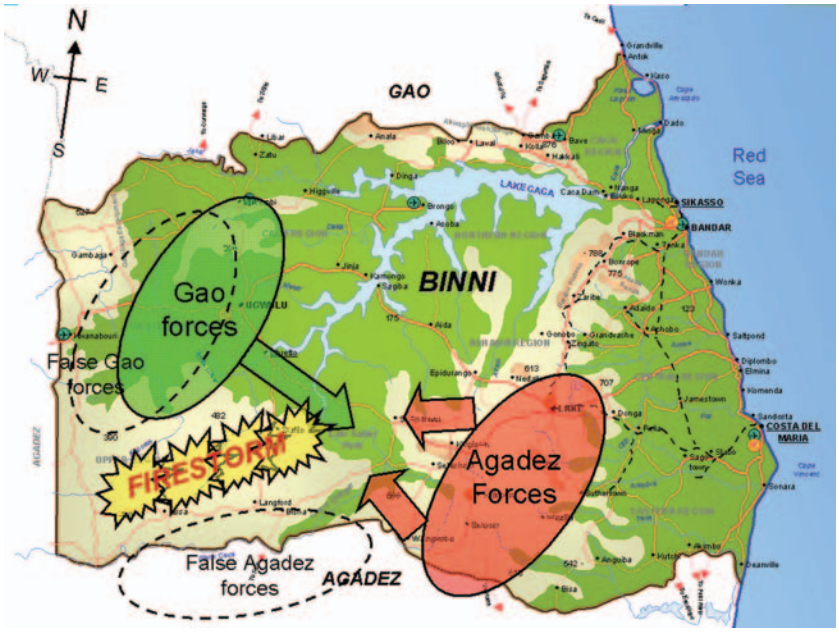


Fig 6. Map of Binni showing firestorm deception. Misinformation from Gao is intended to displace the Firestorm to the west, allowing Gao and Agadez forces to clash in the region of the Laki Safari Park.

Overall, the demonstration showed

- the grouping of agents into policy-governed domains
- the linking of agents and 'agent wrapping' of legacy military systems such as the UK's Master Battle Planner, enabling it to receive dynamic updates (figure 7)
- the extraction and import of publicly available data on the web
- the detection and control of hostile agents
- visualization of the current state of operations via I-X (Intelligent Technology Project) Process and Event Panels [19]
- support for coalition shared awareness.

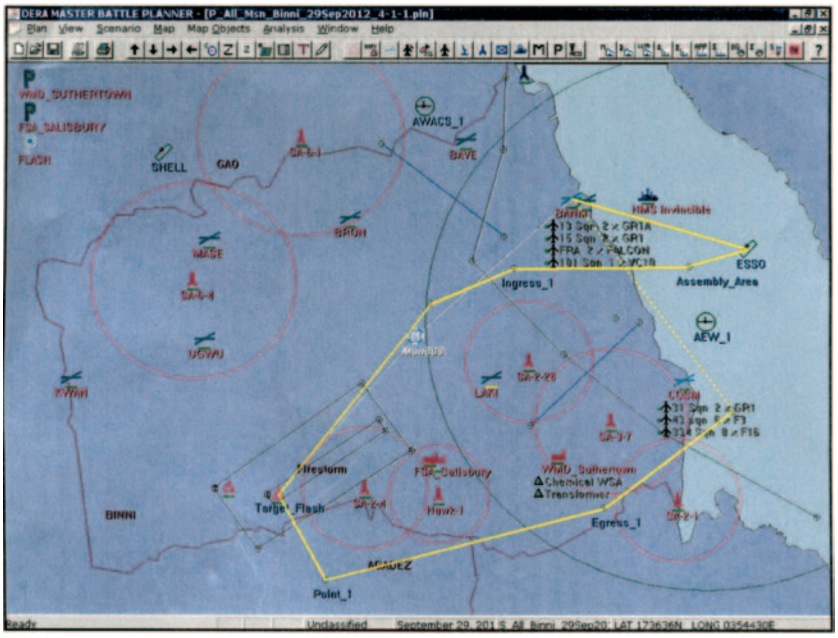


Fig 7. Master Battle Planner map display of Binni, Gao and Agadez showing information gathered from an agent-enabled coalition infrastructure. A selected mission is highlighted, proceeding from an airbase (BANM) to refuelling tanker (ESSO) to the target via waypoints and airspaces, and back to base by a different route.

CoAX Binni 2001 demonstration: dynamic execution phase

The events of the CoAX Binni 2001 demonstration moved on from the initial planning and information gathering phase to a specific day and time in the execution phase, involving the monitoring, battle management and short-notice re-planning associated with coalition operations [6].

The Firestorm mission was planned in detail and aircraft were prepared for their missions. However, the news media broke a story that wildlife in an important safari park in Binni might be in danger as the park overlapped the Firestorm area. With only an hour to go, the UN Secretary General's Special Representative to Binni asked the Coalition Force Commander (CFC) to guarantee that wildlife would not be at risk from the Firestorm operation. Dynamic information gathering and information feeds using agent technology were used in real time to communicate the positions of some of the large mammals at risk. After consideration, it was decided to continue with the Firestorm operation but to re-plan as necessary to avoid risk to wildlife. Firestorm targets were adjusted in time, or secondary targets selected as necessary, for the first wave of firestorm bombing. The impact of these changes on the coalition's medical and humanitarian operations was automatically detected, and unintended conflicts between disjoint coalition operations were avoided. Lastly, Agadez fighters launched high-value asset attacks against the coalition forces; these were detected and important monitoring agents were moved to other computational platforms as the monitoring aircraft regressed.

This demonstration showed newly-arrived agents integrated into domains at short notice, introduced additional time-critical agent functionality such as de-confliction of air task messages and updates exported from master battle planner, run-time re-configuration, and integration of remote, near real-time sensor feeds and unclassified information from the Internet.

CoAX Binni 2002 demonstration: dynamic coalition reconfiguration

The events of Binni 2002 followed those of 2000 and 2001, and began with an attack on an Australian monitoring ship in the Red Sea by two Agadez submarines. The neighbouring country of Arabello (figure 1) was prompted by the attack to offer its ASW capabilities. This offer was quickly accepted and Arabello's sensors were rapidly linked into the coalition's C4I agent framework. Subsequent coalition ASW activities forced Agadez to back down and return to peace talks with Gao at the UN. This scenario is described in more detail next to highlight the key role played by agent technologies.

Submarine attack

Following its unsuccessful fighter attack, Agadez ordered two submarines in the Red Sea to attack an Australian monitoring ship (HMAS Coonawarra). The status of the Coonawarra was monitored by onboard agents, which detected flooding and electrical fire in the engine room and damage to the helideck. They generated an alert, which was sent up the chain of command, in accordance with the agents' standard operating procedures (SOPs) to the Australian and Coalition Force Maritime Component (CFMC) HQs.

On the Coonawarra, the Captain's agent-enabled C4I included a Process and Event-handling Panel (figure 8). I-X Process Panels understand the coalition's organizational structure and can support inter-human and inter-agent messaging in a structured form concerning issues, activities, constraints and reports [19]. They can offer SOPs for

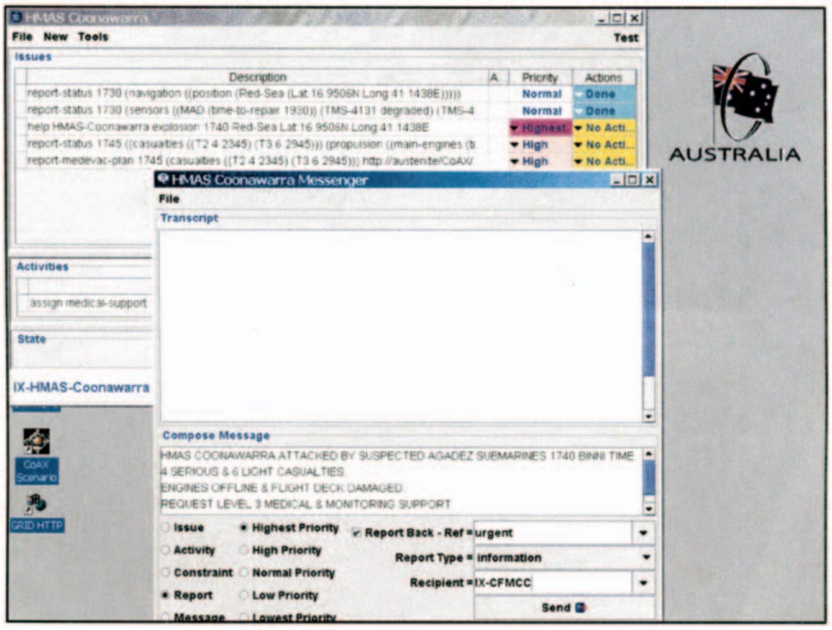


Fig 8. The foreground I-X Process Panel shows a message generated automatically by agents on board the Coonawarra in response to the submarine attack. The panel is aware of the coalition structure and suggests a recipient accordingly. The panel in the background shows ongoing issues being reported to the Captain, for example status reports from agents on the ship.

responding to events or making requests. In this case, the Captain used the panel to report on the attack, the ship's status and the resulting ten casualties. This report was sent automatically to the relevant HQs. Owing to the basic facilities on the ship, the Captain requested minimum level 3 medical support and assistance with medical monitoring.

The report was passed up the command chain to the coalition force (CF) HQ where an event panel was used to delegate the immediate aid and medical assistance tasks to the nearest ship with level 4 medical facilities, the USS C Powell. The Powell acknowledged; this confirmation was sent back through the various panels.

This vignette showed how interface agents working collaboratively across the software agent network reported a submarine attack on an Australian ship to the coalition C4I infrastructure. The agents on the Coonawarra were able to respond to the attack and the damage that was caused by reconfiguring themselves to take account of the information sources that were no longer available. This supports the NEC core themes of full information availability and resilient information infrastructure. Mixed initiative (human-agent interaction) messaging was used to request medical assistance and tasking, and responsibilities were reallocated. This supports the core themes of shared awareness and flexible working.

Casualty information

Australian personnel wore medical tags that monitored their well-being and sent data to a medical database on the ship. To aid the Australians, system administrators at CF HQ were tasked to deploy medical monitoring agents to the Coonawarra. These agents interrogated the medical database on the ship and made the information available in near real-time to the medics on the USS C Powell and at the Australian, CFMC and CF HQs. This was achieved using KAoS policy administration tools, which dynamically reconfigured the agents with new mobility policies and thus permitted them, while still running, to move to where they were needed.

A monitoring agent then reported that one casualty was in crisis. Medics stabilized the critical patient and recommended immediate evacuation to a Level 3 medical facility. The coalition's de-confliction / optimization agent service determined that there was a logistics supply helicopter already *en route* that could also pick up casualties. As a result, the critical patient received attention 30 minutes earlier than would have occurred without this collaborative re-planning.

In this vignette, security permissions were set up and mobile medical monitoring agents were dispatched. Using services defined by the grid mobile agent system, they moved from one type of agent environment to another and still performed as before. The medical evacuation flight was de-conflicted as a result of agent-instigated alerting. The agents de-conflicted and optimized the plan by being able to access and exploit synergies in coalition-wide open information. This supports NEC core themes of flexible working and synchronized effects. The agent behaviour in cyberspace that was triggered by these events was monitored and visualized as part of full-spectrum dominance, which supports the core theme of shared awareness. It is this ability to adapt to the ever-changing realities of conflict at run-time that makes software agents so useful.

Arabello joins coalition

The Coonawarra had novel magnetic anomaly detection equipment, and had been releasing the resulting information to the coalition, but this capability was seriously degraded by the attack. The nearby country of Arabello was identified as a possible ally to fill this information gap. Wishing to support a trading partner under direct attack, and seeing the risk to shipping from Agadez submarine activity, Arabello asked to join the coalition and offered its ASW capability, an underwater sensor grid. The coalition used its agent performance evaluation tool to examine this capability and verify it as suitable.

Coalition system administration staff provided a 'Coalition Agents Starter Pack"[20] to Arabello to bring them up to speed on coalition operational and technical matters, and to set up secure, selective information interoperability between the coalition and Arabello. This pack contained scenario information, agent wrappers, process and event panels, policy and domain management capabilities, and set-up and configuration instructions.

To avoid sharing more intelligence than necessary, Arabello created a policy restricting its agents only to provide reports on Agadez submarines, and only to coalition agents. This was an example of restricting communications by message content, rather than just by the domain of the sender and receiver [14,21]. Policy information was represented using DAML, which, combined with KAoS components, provided powerful policy reasoning, de-confliction and enforcement capabilities. Any conflicts between policies and possible resolutions were displayed graphically for system administration staff.

Once interoperability with Arabello was established, a formal tasking was sent from the CFC via the Process Panels, requesting the sensor data. The Arabello agents did not need to know what other agents would require data; they made its availability known via a matchmaker agent so that other agents could find data dynamically. This approach enabled services and capabilities to be advertised and withdrawn as circumstances changed.

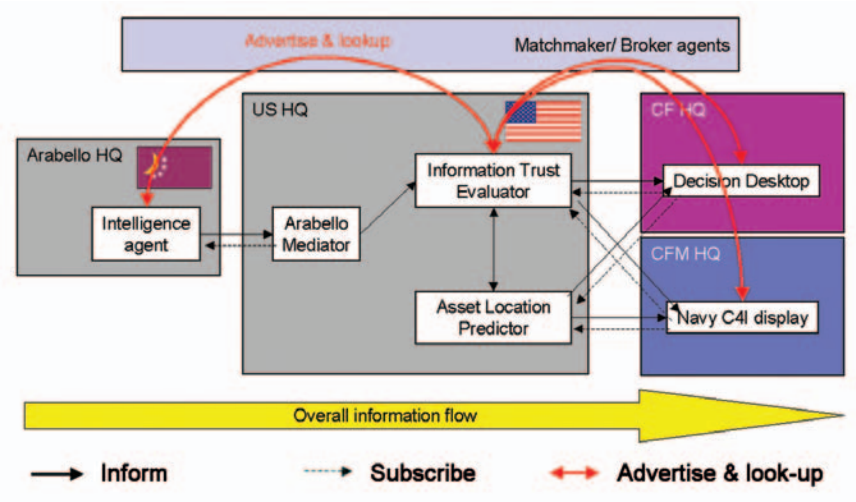


Fig 9. Secure and selective integration of sensor data from a new coalition partner. Data are fused and used to predict future submarine locations, and delivered to C4I display tools. The mediator agent is rapidly generated using an agent toolkit. Links between agents are created dynamically through look-up and advertisement –they are not hardwired.

In this vignette, Arabello joined the coalition after its alternative ASW feeds were validated as suitable. It used the starter pack to make selected parts of its agent-based underwater sensor grid capabilities visible to coalition members as an intelligence service. The service was advertised and used by coalition HQs as required. This supports the core themes of agile mission groups, resilient information infrastructure and fully networked support. This part of the demonstration showed how a completely unexpected, unprepared, partner was integrated into the coalition command structure at short notice.

Agents enable sensor fusion

Next, the CFMC Commander tasked the US HQ to acquire sensor data from Arabello, to translate it, and fuse and collate it with existing coalition information. This was delegated to the system administration staff in the various HQs. They used an agent creation toolkit (Interoperable Intelligent Agent Toolkit [22]) that lets non-programmers compose agent behaviours graphically and dynamically. Without these capabilities, the interface negotiation, code development and system integration could have taken months to achieve the same level of interoperability. An agent was created to act between the Arabello sensor agent and the US fusion agent. This 'mediator' agent could translate between the different forms of XML used to represent sensor data by members of the coalition, and thus pass data from Arabello to the US domain (figure 9).

Agent tools in the US domain provided the fusion service for the coalition. Before the submarine attack, the fusion service had been collating information from satellites (available twice daily), sundry radar returns (frequent but often unreliable), unmanned autonomous image feeds (asynchronous and often unreliable) and from the Australian magnetic anomaly detection (reliable and continuous). After the attack, Arabello provided historical data and an ongoing and moderately reliable feed. An 'information trust evaluator' agent fused sensor reports from the Arabello mediator agent with existing sources, taking into account sensor reliability and trust. The fused sensor data were made available to all agent-enabled C4I tools, such as the CFC's Decision Desktop (figure 10).

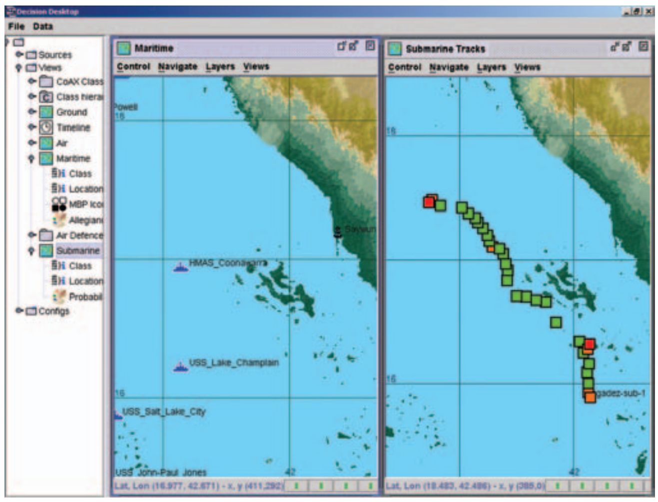


Fig 10. Submarine contacts from Arabello are delivered to the Decision Desktop C4I visualization tool. The panel to the right shows that the commander has chosen to display them according to their confidence levels. These could also be added to the standard maritime display.

Next, the warfighters needed to predict the likely positions of the Agadez submarines to determine their responses. The US possessed several 'asset movement' agents, which could access the coalition-wide fused sensor data, calculate likely predicted locations of the Agadez submarines, and provide output to C4I agent systems such as the CFMC HQ displays.

In this vignette, Arabello's sensor grid information was made available to the coalition by creating a 'go-between'agent that enabled Arabello's intelligence agents to talk to the US fusion service. Arabello's feed was collated with the others available to the coalition, and a trust evaluator agent dynamically selected the best information and forwarded it, re-assessing the value of the feeds, and switching sources appropriately as time passed. This supports the core theme of full information availability.

Next, the Agadez submarines' locations were predicted and then displayed on the various coalition C4I systems. This was achieved by interaction among the heterogeneous agents. Using these techniques, information was published and made available to be picked up by any decision makers, as they demanded it, and displayed on their C4I systems in the form they required. This supports the NEC core theme of shared awareness.

Dissemination of information and countermeasures

Once the positions of the Agadez submarines were predicted, coalition ASW forces had to locate them exactly and box them in with patrol boats and sonobuoys. To help Arabello with this task, the coalition provided a feed from the magnetic anomaly sensor on the Coonawarra, now operational again. However, the Australians did not want to reveal the full capabilities of the sensor to Arabello, so they provided degraded images by setting appropriate agent policies using the KAoS policy administration tool, and Nomads filtering and transformation policy enforcement mechanisms.

The policy dynamically lowered the resolution of the sensor data before sending it to Arabello (figure 11). Other forms of transformation were possible, including introducing a time lag (non real time) or reducing the update rate. Filtering of sensitive data (eg, the location of a US submarine) could also be implemented. Suri *et al* provide more detail on how these capabilities worked in the CoAX context [21].

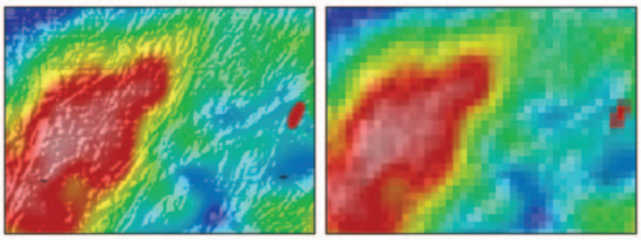


Fig 11. On the left are shown the original sensor data from the Coonawarra's magnetic anomaly detection equipment. On the right are the same data after being dynamically transformed and downgraded for release to the coalition.

The Arabello Maritime Commander used an agent-enabled planning system to help him to gather information, select targets, identify resources to use, communicate with his subordinates and issue orders. This mixed-initiative tool allowed the commander to manipulate the military objects (ships, targets, etc) directly on the screen and arrange assets to achieve synchronized effects. The agents sensed these interactions, and fetched and updated the required information in the background, acting as part of the mission team. Subsequently, because of the coherent activity by the coalition, Agadez returned to the negotiating table.

In this part of the scenario, agents dynamically maintained the interconnection and interoperability between relevant information feeds and a service that output a stream of predicted Agadez submarine positions. Agent policies were used to control the dynamic filtering of information before passing it to Arabello. This supports the core themes of full information availability and resilient information infrastructures. Interface agents supported warfighters as they assembled information to make decisions and deploy countermeasures against the Agadez submarine. This supports the core themes of agile mission teams, effects-based planning and synchronized effects.

5 CONCLUSIONS

Assessment of CoAX

The overall goal of CoAX was to show that an agent-enabled infrastructure significantly aided the construction of a coalition command support system and improved its effectiveness. Referring to the specific operational and technical objectives highlighted in section 1, we deduce that good progress was made towards achieving the aims of CoAX.

Objective a)

There were many examples in the CoAX demonstrations of agents facilitating information sharing between disparate systems. For example, the CoAX 2000 demonstration included the agent-enabled inter-operation of real military systems, namely the Master Battle Planner and the Consolidated Air Mobility Planning System.

Objective b)

Specific instances of adaptive responses at run-time include the re-planning of air missions in CoAX Binni 2001, because of the need to avoid large mammals in the Laki Safari Park, and Arabello joining the coalition in CoAX Binni 2002.

Objective c)

In CoAX Binni 2002, the loosely-coupled agent architecture allowed Arabello's ASW information to be advertised to members of the coalition, who were then able to access it when required.

Objective d)

The provision of 'downgraded' Australian sensor data in CoAX Binni 2002 provided an example of selective information sharing. The KAoS policies and domain structures controlled agent behaviour throughout all the demonstrations, facilitating coalition agent interaction and preventing defective, malicious or poorly-designed agents from impeding coalition objectives.

In the CoAX experiments, running software agents and the CoABS grid software was not found to impose a noticeable overhead on processing or communications. In general, the flexibility of agent-based systems means that they are likely to be able to adapt to varying levels of resource availability, and policies can control their utilization of resources.

Relevance to NEC

There are several reasons why agents can support NEC, making them potentially useful during conflict. First and foremost, because their behaviour is not fixed at 'design-time', they enable military commanders to behave unpredictably – to 'wrong-foot' an opponent. Software agents can be dynamically reconfigured, supporting the NEC core themes of flexible working and agile mission groups.

Secondly, an opponent will impose unpredictable events and outcomes on the battlespace, so it is impossible to plan all requirements in advance. Hence, commanders must be able to adapt to the military imperative at run-time – the command systems must not constrain users' scope of actions. Hence, as software agents can be tasked according to the circumstances, they support the core themes of synchronized effects and effects-based planning.

Next, unlike traditional software that is reactive, agents are capable of being proactive and predictive. Although their autonomy and intelligence give them much more freedom, the actions of the agents and the flow of information among them are kept under strict control by human administrators through policies that are enforced in the domains to which agents belong. Agents can adapt to changing circumstances at run-time, and can use messages and events to act as triggers – hence they are not tightly constrained at design time to what they do. Indeed, their ability to 'self-heal' at run time makes them robust in the face of a real battlespace that is event-driven, high-tempo, short timescale, uncertain, diverse and dynamically varying. Consequently, software agents support the core themes of full information availability and resilient information structure.

Lastly, software agents can work with humans in a so-called mixed initiative manner such that, as the humans click, type and speak, they are triggering agent actions. Agents can sense certain real-world events and report back to the humans. The humans and agents work as a collaborating distributed team [15]. The activities are not determined at 'design-time' (over-engineered and brittle) but are free flowing and natural. In this case, software agents are supporting the core themes of shared awareness and fully networked support.

Strengths and weaknesses of agent technology

The generic main strengths of the agent paradigm are that it offers [23,24]:

- a powerful metaphor for conceptualizing complex systems; it is natural to model complex systems in terms of self-supporting agents that provide services and undertake tasks on behalf of other agents, systems and users.

- distribution of control. Agents support a distributed, heterogeneous model of computing. Agent communication languages provide the means for agents to interoperate in a seamless fashion, irrespective of where they exist in the environment. Real-world problems are overwhelmingly distributed in nature.

- a natural means of exploiting and controlling concurrency. Multi-agent systems comprise asynchronous processes that communicate by passing messages. Agent co-ordination strategies and policies control how agents interact and the actions they are allowed to perform.

- a mechanism for leveraging open systems with heterogeneous computing platforms and disparate programming languages. A key advantage of agent-based computing is the inter-operation of disparate agents and systems.

- the ability to support global services marketplaces. The current trend towards viewing organizations as service providers is likely to become ubiquitous. With this view, software agents will represent the individuals, departments and organizations that provide services.

- a natural computational model for pervasive computing. As the IT world creates environments that are saturated with computing and wireless communications, it is increasingly likely that agents will be seen carrying out functions and providing services on embedded devices and systems.

Despite this promise, however, there are some current weaknesses in implementation [23,24]:

- tool support. Developing distributed computer applications is a highly skilled activity, as is developing multi-agent systems. Currently, there is a marked lack of tools that assist in the development, testing, performance monitoring and debugging of agent applications. Achieving good performance relies on careful design and implementation.

- agent component libraries. One of the distinct advantages of object-oriented development is the availability of high-quality third-party libraries of reusable components. There is now a clear requirement for agent libraries and frameworks that support, for example, intra- and inter-agent communication, planning, knowledge representation, reasoning, negotiation, etc.

- environments. The uptake of agents will require the development of robust, secure and inter-operable run-time environments that provide agents with the 'life support' they require [25]. For example, 'end to end' interoperability requires some form of shared semantics, the ability to deal with multiple agent communication languages and operations across firewalls.

Future directions

Tools such as the prototype Coalition Agents Starter Pack [20], developed for the CoAX 2002 demonstration, could form the basis for future coalition warfare programmes and could be evaluated within the UK's experimental NEC programmes such as the Experimental Network Integration Facility (now re-named NITEworks). Areas requiring further research and evaluation include richer descriptions of agent services and capabilities (based, for example, on semantic web technologies) leading to dynamic, automatic and trusted composition of services across the battlespace, and agent-based architectures that are secure and resilient in the face of physical and information-based attacks.

Acknowledgements
We are greatly indebted to all those who worked on CoAX – the CoAX web site [8] contains a complete listing of all participants. We would also like to thank Dan Daskiewich (Air Force Research Laboratory), Jim Hendler (DARPA and University of Maryland), RAdm Lee Kollmorgen (Naval Research Laboratories), Capt David Marsh (Air Force Research Laboratory), Rick Metzger (Air Force Research Laboratory) and Lt Cdr Dylan Schmorrow (DARPA) who played a key role in instigating and supporting CoAX. QinetiQ work was carried out as part of MoD's research programme and also part funded by DARPA. Apart from DSTO Australia, the other projects that participated in CoAX were sponsored by DARPA and managed by the US Air Force Research Laboratory. DARPA, the US Army, the Office of Naval Research and NASA sponsored Jeffrey Bradshaw's work on KAoS policy-based agent domain services. The US Government, the University of West Florida, the University of Edinburgh and BBN Technologies are authorized to reproduce and distribute reprints of the published article for their purposes notwithstanding any copyright annotation hereon.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing official policies or endorsements, either expressed or implied, of the UK MoD, DARPA, the US Government, QinetiQ, University of Edinburgh, University of West Florida or BBN Technologies.

References

1 Jennings N R, Sycara K and Wooldridge M. *A roadmap of agent research and development.* Autonomous Agents and Multi-Agent Systems **1** 275 (1998).

2 Bradshaw J (editor). *Software Agents*. AAAI Press / MIT Press, Cambridge, Massachusetts (1997).

3 Bradshaw J (editor). *Handbook of Agent Technology*. AAAI/MIT Press, to be published (2003).

4 Bradshaw J M *et al* (editors). *Software Agents for the Warfighter.* ITAC Consortium Report. Cambridge, Massachusetts, AAAI Press/The MIT Press. (2002).

5 Networked Enabled Capability flyer, version 5.0, 18 October 2002.

6 Allsopp D N *et al*. *Coalition Agents Experiment: Multiagent Cooperation in International Coalitions,* IEEE Intelligent Systems May/June **17:3** 26 (2002).

7 TTCP web site: http://www.dtic.mil/ttcp.

8 Coalition Agents Experiment web site: http://www.aiai.ed.ac.uk/project/coax.

9 Control of Agent-Based Systems web site: http://coabs.globalinfotek.com.

10 Rathmell R A. *A Coalition force scenario 'Binni – gateway to the Golden Bowl of Africa'*. In Proceedings of the International Workshop on Knowledge-Based Planning for Coalition Forces (editor A Tate) pages 115-125, Edinburgh, Scotland, 10th–11 th May 1999. Available at: http://binni.org.

11 Binni web site: http://binni.org.

12 Jennings N R. *An agent-based approach for building complex software systems.* Communications of the ACM **44:4** 35 (2001).

13 Bradshaw J M *et al*. *KAoS: towards an industrial-strength open agent architecture.* In Software Agents, AAAI Press / MIT Press, Cambridge, Massachusetts (editor J M Bradshaw) 375-418 (1997).

14 Bradshaw J M *et al*. *Representation and reasoning for DAML-based policy and domain services in KAoS and Nomads*. Proceedings of the Autonomous Agents and Multi-Agent Systems Conference (AAMAS 2003). Melbourne, Australia, ACM Press, New York (2003).

15 Bradshaw J M *et al*. *Making agents acceptable to people.* In Handbook of Intelligent Information Technology. IOS Press, Amsterdam, Holland (editors N Zhong and J Liu) (2003).

16 Semantic web activity statement web site: http://www.w3.org/2001/sw/Activity.

17 Berners-Lee T, Hendler J and Lassila O. *The Semantic Web*. Scientific American (2001) available at: http://www.sciam.com/2001/0501issue/0501bernerslee.html.

18 The DARPA Agent Mark-up Language web site: http://www.daml.org.

19 Tate A, Dalton J and Stader J. *I-P2: Intelligent Process Panels to Support Coalition Operations*. In Proceedings of the Second International Conference on Knowledge Systems for Coalition Operations (KSCO-2002), Toulouse, France, 23-24 April 2002. Available at:http://i-x.info/documents/2002/2002-ksco-ip2.pdf

20 Coalition Agents Starter Pack available at: http://www.aiai.ed.ac.uk/project/coax/demo/2002/coalition-starter-pack.html.

21 Suri N *et al*. *DAML-based policy enforcement for semantic data transformation and filtering in multi-agent systems.* In Proceedings of the Autonomous Agents and

Multi-Agent Systems Conference (AAMAS 2003), Melbourne, Australia. ACM Press, New York (2003).

22 Interoperable Intelligent Agent Toolkit web site: http://www.atl.external.lmco.com/overview/programs/IS/I2AT.html

23 Kirton M J and Jennings N R. *Software agents and interoperability.* QinetiQ/KIS/SEB/CR020183/1.0 (2002).

24 Millington P. *Exploitation of agent technology.* Logica report, reference EC26904:3.1 (2002).

25 Bradshaw J *et al*. *Terraforming cyberspace*. IEEE Computer **34:7** 48 (2001).

Glossary

AIAI	Artificial Intelligence Applications Institute (at the University of Edinburgh)
ASW	Anti-Submarine Warfare
CF	Coalition Force
CFC	Coalition Force Commander
CFMC	Coalition Force Maritime Component
CISP	Communications Information and Signal Processing
CoAX	Coalition Agents Experiment
CoABS	Control of Agent Based Systems
C4I	Command, Control, Communications, Computing and Intelligence
DARPA	Defense Advanced Research Projects Agency
IHMC	Institute for Human and Machine Cognition (at the University of West Florida)
I-X	Intelligent Technology Project
KAoS	Knowledgeable Agent-Oriented System
NEC	Network Enabled Capability
SOP	Standard Operating Procedure
URI	Uniform Resource Identifier
XML	Extensible Mark-up Language

QinetiQ Ltd, Malvern Technology Centre, Malvern, Worcs WR14 3PS
Kirton@signal.QinetiQ.com

NEC social and organizational factors

John Holt
HVR Consulting Services Ltd

Abstract
NEC aims to connect sensors, decision-makers and weapons reliably so that information is exploited better, to deliver synchronized effects. This paper concentrates on the factors that will greatly reduce C2 decision time by providing shared information, to achieve shared awareness and collaborative decisions, facilitating decision-making at all levels. The development of a set of processes to achieve such a high level of performance will need to reflect the relevant human decision-making and social factors fully. This paper describes and evaluates the impact of social factors on NEC, particularly focussing on the development of working relationships within a disparate, multi-nation force.

1 INTRODUCTION

UK and US forces are moving to a new concept of networked forces such that sensors, decision-makers and weapons are connected to a network that will allow free passage of information. 'It is intended that this will lead to greater shared awareness, enabling a degree of self synchronization, leading to increased speed of command and tempo, and enhanced lethality and survivability.'[1].

This new way of working is referred to in the US defence community as Network Centric Warfare (NCW). The concept has been modified in the UK and is referred to as Network Enabled Capability (NEC). Previously, similar developments in C2 systems were considered under various digitization projects. As most of the social and organizational factors are common across these areas, the terms NCW and NEC are used interchangeably in this paper.

2 BACKGROUND

In NEC behavioural and social research, two major perspectives have emerged. The first has focussed on cognitive and social factors, particular 'organizational sense-making' [2, 3]. This is a "collaborative process influenced by social and cognitive factors that seeks to reconcile the framing of problems and decision points among a set of operational stakeholders". It provides a very useful description of the steps in the process of developing shared understanding in C2 systems and has been used to identify requirements for a range of tools to develop the necessary steps, including story-telling, visualization tools and knowledge mapping (to know what knowledge can be found in an organization, and where it can be found). These and similar approaches have been at the root of a number of NCW/ NEC frameworks that have been developed to enhance understanding and to provide metrics, an example of which is given in the NCW framework section below.

An alternative perspective on social factors has been developed in a dissertation on NEC cultural factors from RMCS Shrivenham [1]. This has highlighted a number of cultural barriers to achieving NEC, from the perspective of current British Army and general cultural theory. From cultural theory, RMCS have identified three layers of issues:

- Layer 1 deals with explicit culture, which is tangible and easy to change (eg, uniforms, processes, Army structure).
- Layer 2 refers to the norms and values of the armed forces that provide context for layer 1 (doctrine, customs, etc). Layer 2 can be changed but the armed forces will be most reluctant to embrace such changes.
- Layer 3 is the implicit culture, the deep-held beliefs about an organization (such as subordination to a superior). These are difficult to identify and change.

Some of the main areas of concern in NEC have been highlighted by the study:

- There is a human propensity to hoard knowledge to preserve power, which runs counter to the requirement for an NEC force to pool its knowledge (probably a Layer 1 cultural issue).
- For NEC to achieve its potential requires decentralization of power so that those on the ground make the decisions. If information has to be passed back up a hierarchy, it will add unnecessary delay. (This may be a Layer 2 cultural issue.)
- Achieving a shared mental model requires working closely together. Dispersion reduces the ability to create such a model, and it is generally assumed that NEC will be implemented in a very dispersed force. (This may touch on both Level 1 and Level 3 issues.)
- Motivation in combat is normally brought about by high morale, discipline and leadership. This is particularly necessary in army close battle, possibly at the expense of relations with other groups. It will be very difficult to achieve in an NEC environment when a commander's intent is merely passed over the network rather than by his being on the spot. (Both a Layer 2 and Layer 3 issue)

These two perspectives have highlighted very different sets of issues. This paper identifies a further set of social factors that are currently not addressed in either perspective, in the area of building up effective working relationships so that knowledge is shared. Research has been drawn from social and organizational psychology where there has been useful survey-based research of digitized information technology in civil environments. The different types of psychology referred to in this paper are shown in figure 1, with the left of the figure being the more individually and the right the more societally oriented. Figure 1 shows that the new areas referred to in this paper, social and organizational, are in the middle, with the two existing areas of cognitive/ social and cultural at each end of the spectrum.

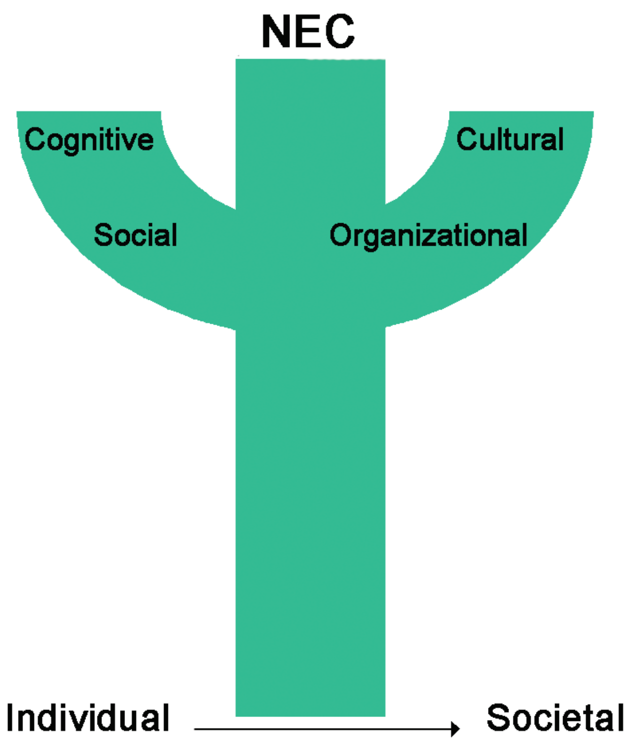


Fig 1. Approaches to psychology referred to in this paper

This paper is the result of a Dstl workshop on NEC social factors, with representatives from Dstl Information Management, QinetiQ Centre for Human Sciences, Surrey University School of Management and Dstl supporting consultants. At this workshop, the author presented the ideas in this paper and received feedback.

The following were the main data sources for this paper:

- recent Surrey University research on the social psychology of organizational networks [4]
- other Surrey University work sponsored by QinetiQ, specifically a survey of FTSE Top 100 companies working in civil digitized systems [5]
- C2 research on cultural factors in multinational headquarters (HQs) [6]
- classic organizational theory on how organizations evolve under high-pressure [7].

In this study, cognitive mapping (a soft operational research method) and a particular NCW framework were used [8]. They are described in this review of the study background. The main section of the paper then describes social factors using the NCW framework.

Description of cognitive mapping

A cognitive map is a set of statements linked by arrows, as shown in figure 2, with concepts represented by the numbered, rectangular shapes (in yellow) and arrows showing causal links, in a hierarchy of low-level concepts leading to high-level goals. Cognitive mapping has been used to link research from many different sources, and greatly facilitated discussion at the workshop. It is used to aid understanding of the relationships between social factors. The package used to generate the maps is Decision Explorer, developed by Banxia. The conventions for understanding a cognitive map are shown in figure 2. The main convention is that an arrow represents a causal link. The numbers are not significant but useful in referring to effects.

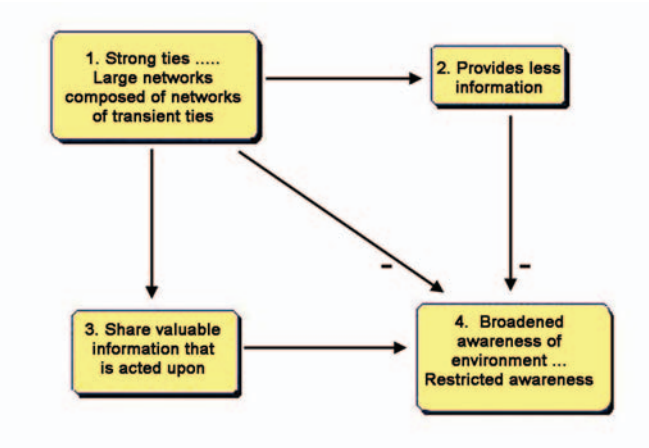


Fig 2. Description of cognitive mapping

- Where it adds clarity, concepts are used with their opposites (bipolar), indicated by dots (eg, 1 and 4). These opposites represent perceived rather than logical opposites (eg, 4 Broadened... Restricted awareness), thus aiding understanding of how the concept is used.
- Where a single concept is given, eg 2, it is assumed that the opposite is purely the negative (eg, does not share valuable information that is acted upon).
- For sequences of bipolar concepts, right-hand pole leads to right-hand pole and left to left (eg, 1 to 2). Thus for 1 to 2, 'Strong ties' leads to 'Share valuable information that is acted upon', and 'Large networks of transient ties' leads to 'Not share valuable information that is acted upon'.
- A negative sign by an arrow reverses this polarity (eg, 1 to 4). 'Strong ties' leads to 'Restricted awareness', and 'Large networks consisting of transient ties' leads to 'Broadened awareness of environment'.

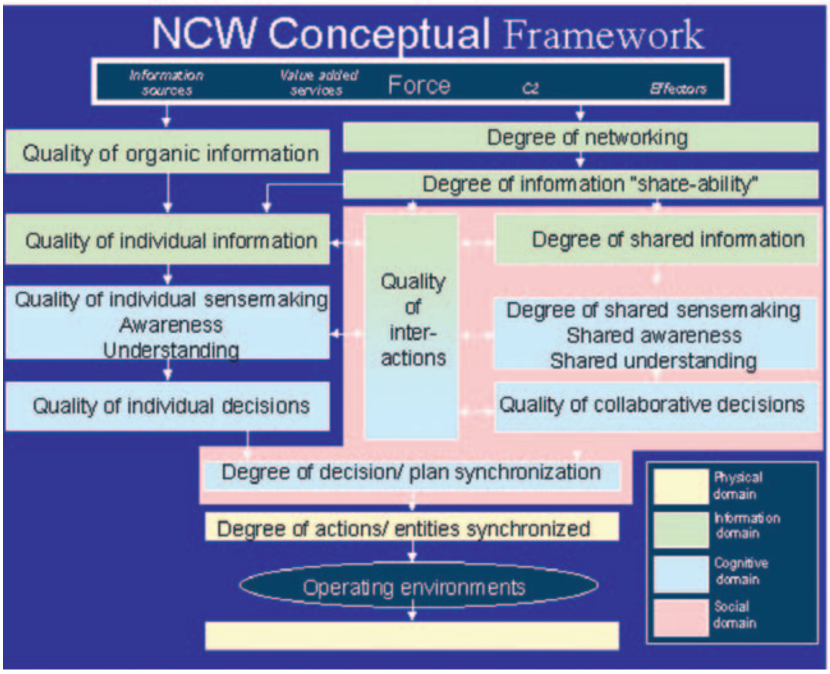


Fig 3. NCW structure

NCW framework

The NCW framework used as the frame of reference for this study is shown in figure 3 [9], and is based on the cognitive and social perspectives. The diagram starts with 'Force', which shows the main components of a force, from information sources through to effectors. The information that comes in is represented as either 'organic' or obtained through 'networking'. The left-hand boxes are processing conducted by individuals and the right-hand boxes refer to collective information. The pink area underlying the right-hand boxes corresponds to the social domain. The main phases for both individual and social processes are 'Information' leading to 'Sense-making', 'Awareness', 'Understanding', leading to 'Decisions'. This paper focuses on the right-hand side of the diagram and the pink area containing the social factors.

3 NCW SOCIAL FACTORS

Having set the background, NCW social factors are now described using the framework in figure 3. Descriptions are given of metrics requirements for each of the NWC factors to provide links to the social factors and aid understanding. Where the social factors provide ways of overcoming cultural problems, this is also indicated in the description. Detailed definitions of the NCW terms referred to are given in tables in Section 5.

Degree of shared information

'Degree of shared information' is the proportion of information that is of common concern across the force that is shared, ie, the proportion of information that should be shared that is actually shared. Its attributes are shown in figure 4.

The RMCS study [1] has shown that there may be a tendency in British Army culture to hold on to information and not pass it on. Figure 5 suggests factors that could help to overcome this potential barrier. From social psychology, the main relational factors leading to shared information (referred to as knowledge transfer) are openness and trust [4].

Degree of sense-making, shared awareness and shared understanding

This is the proportion of individuals across a force who have the required level of awareness. The cognitive component is well described in [2]:

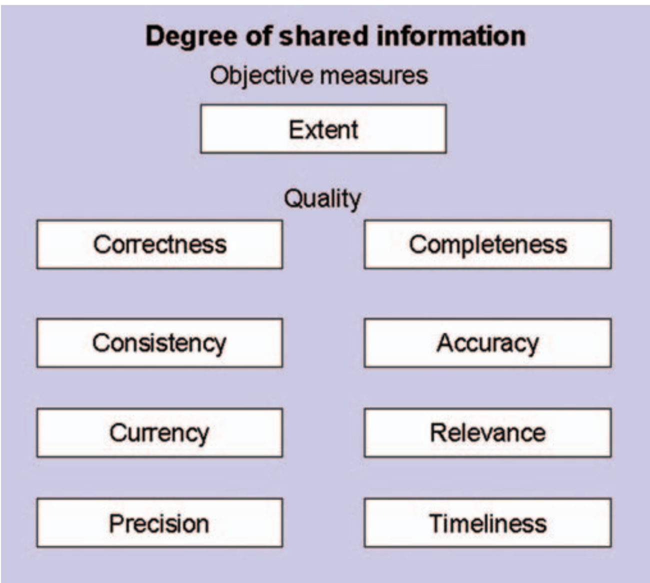


Fig 4. Degree of shared information

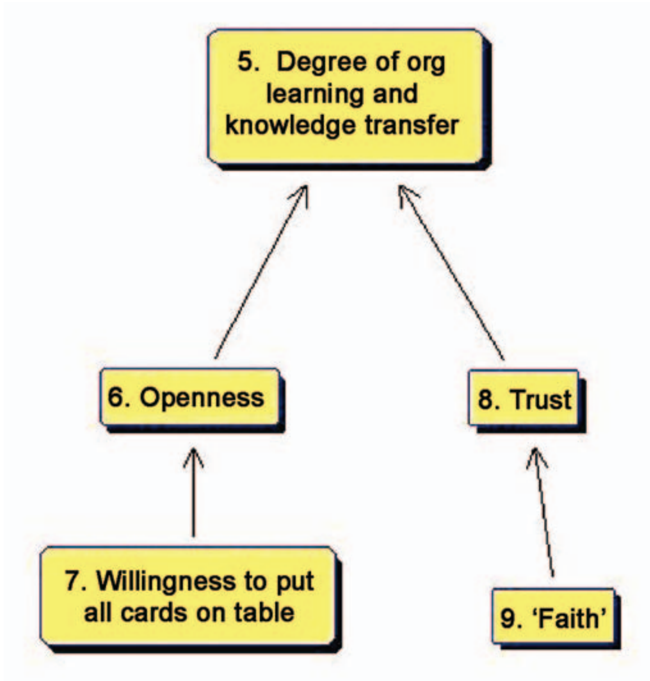


Fig 5. Degree of knowledge transfer

"The implication is that commanders and participants of command teams need to share experiences and need to have social interaction to become informed. The transference of symbols from one to another is not sufficient to transfer a mental construct from one person to another as the mental construct is changed as it is represented by the symbols." Figure 6 shows the metrics factors. Note that the same metrics are used for degree of shared information and quality of interactions.

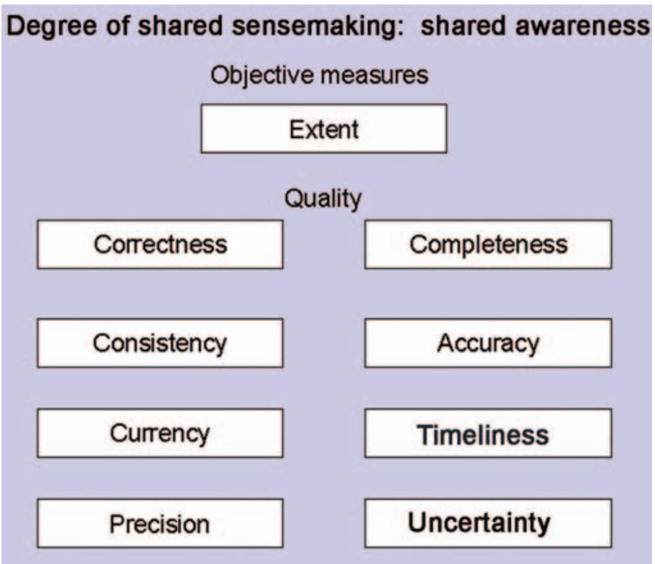


Fig 6. Degree of shared sense-making; shared awareness

The RMCS cultural study referred to a tendency to hold on to information. Concepts from social psychology [4] show what is required for groups to build up relationships so that they will share important information. As shown in figure 7, strong relationships lead to information that is acted upon, as well as broadened awareness of the outside world. Strong ties are developed through frequent interaction, shared history and a willingness to share confidence.

Figure 8 shows that there is also a downside to strong ties, that over time they lead to fewer novel insights as both parties get to know each other. They also require maintenance as relationships need to be cultivated, and hence there is a cost involved in terms of time spent. Concept 17 in figure 8 shows the effect of an alternative strategy, developing relatively large numbers of indirect ties as a way of countering many of the negative factors. This provides less information than in-depth ties, and they are more costly than transient ties, but they do not have the problem of losing insights as familiarity increases. Thus for NEC/NCW, it is necessary that ties are cultivated that maximize the information that is shared but do not have a high overhead in maintaining links.

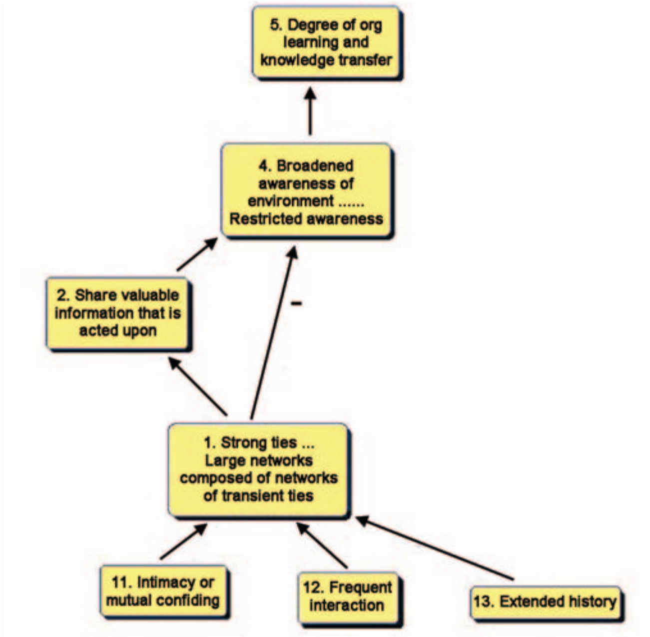


Fig 7. Degree of shared sense-making, shared awareness and shared understanding

Quality of collaborative decisions

This is the proportion of a force that should be involved in a decision that is actually involved (ie, the level of collaboration to achieve the best possible decision). Also of concern in any assessment is the objective quality of the decision that is produced. Figure 9 shows the metrics factors for quality of collaborative decisions in three main parts, 'objective measures', 'fitness for use' and 'agility'.

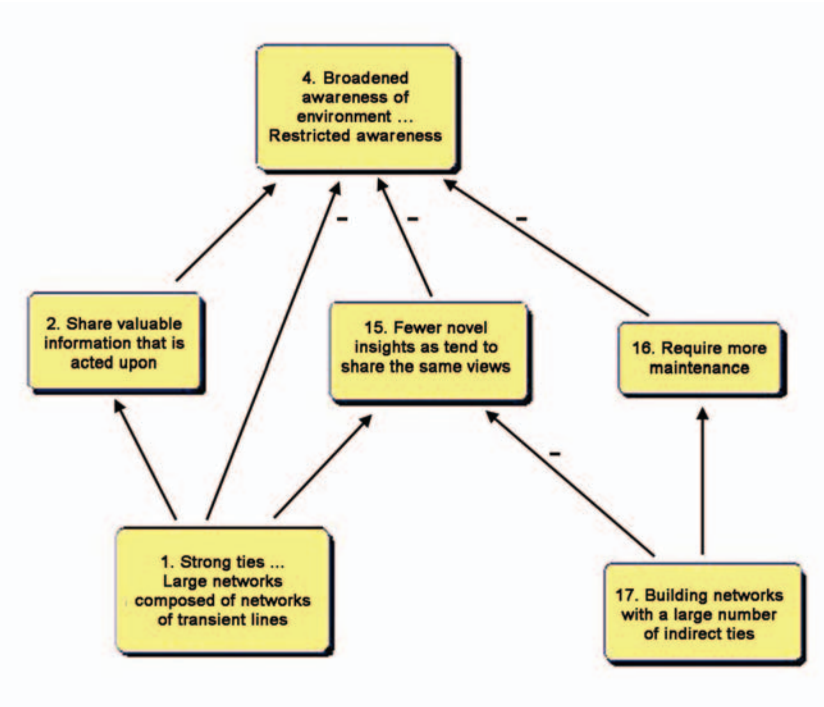


Fig 8. Degree of shared sense-making, shared awareness and shared understanding continued from figure 7.

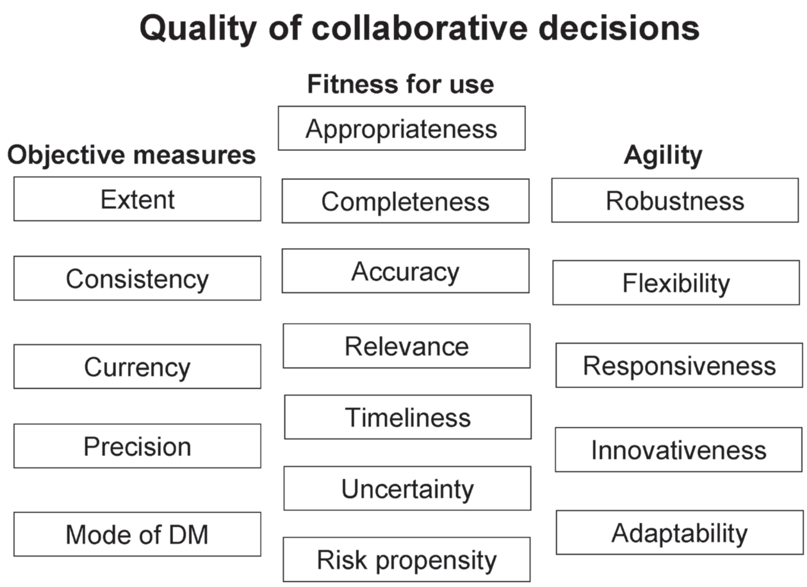


Fig 9. Quality of collaborative decisions

The main social factors for collaborative decisions, from a survey of digitized businesses [5], are shown in figure 10. There is a degree of commonality between figures 9 and 10, with the main concepts being ‘agility’ and ‘situation awareness’. In agility, the speed of decision in particular was seen as a potential critical success factor. For NCW, ‘situation awareness’ is covered under ‘awareness’ and is differently placed (it comes earlier in the decision cycle).

In the civil domain, situation awareness is achieved by applying appropriate technology, which may be quite disparate (examples quoted in the survey were data warehousing –the use of digitization techniques to identify new market places). Note that, in the civil domain, ‘good management does not allow technology to control”. This would be true in the military domain also.

Quality of interactions

This factor is concerned with the extent of force entities actively sharing information, and

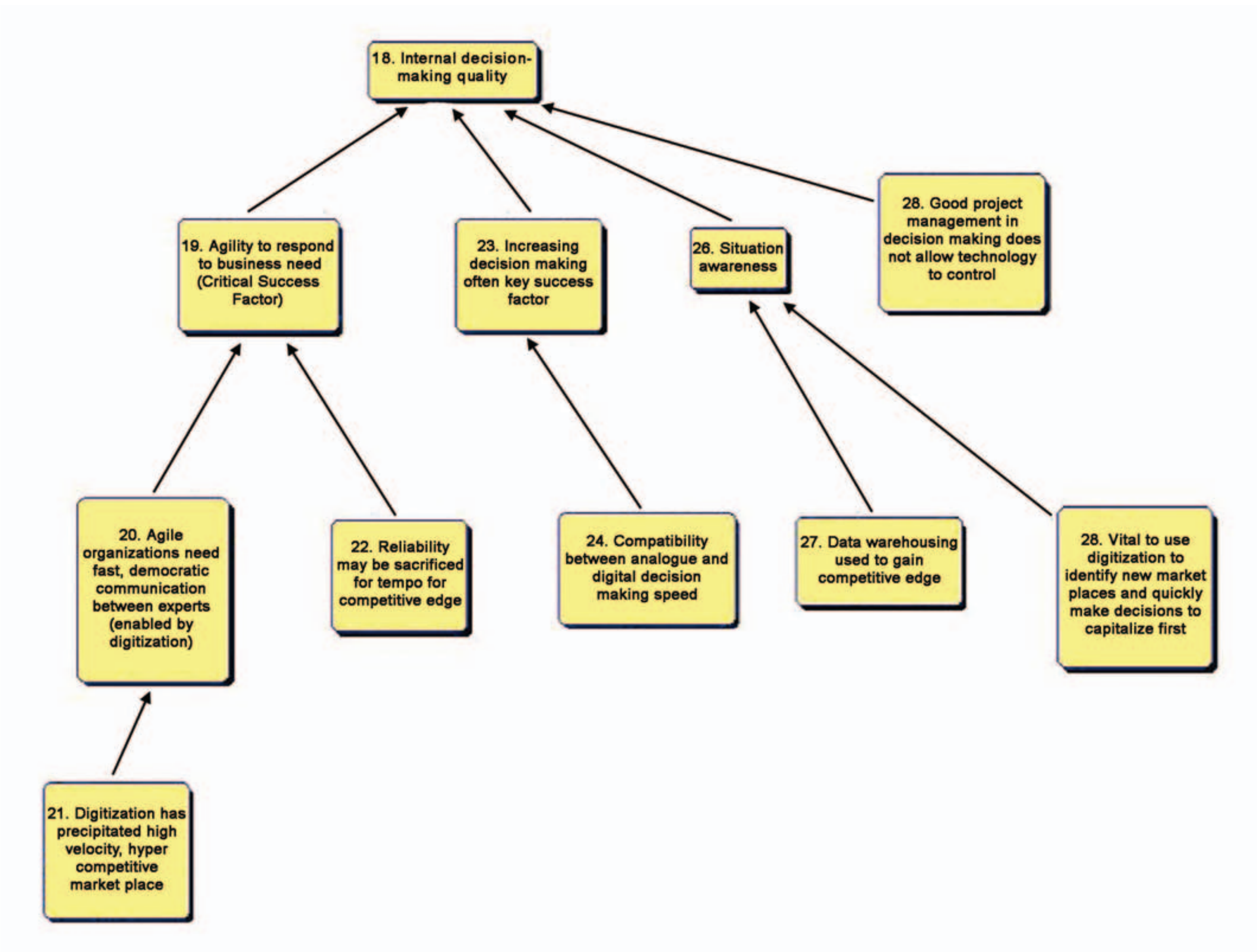


Fig 10. Quality of collaborative decisions in the civil domain

developing awareness, understanding and/or making decisions (developing plans), in a collaborative fashion while working together toward a common purpose [9].

Figure 11 shows the main characteristics of 'quality of interaction' (divided into 'characteristics of interaction', 'individual characteristics', 'organizational characteristics' and 'organizational behaviour').

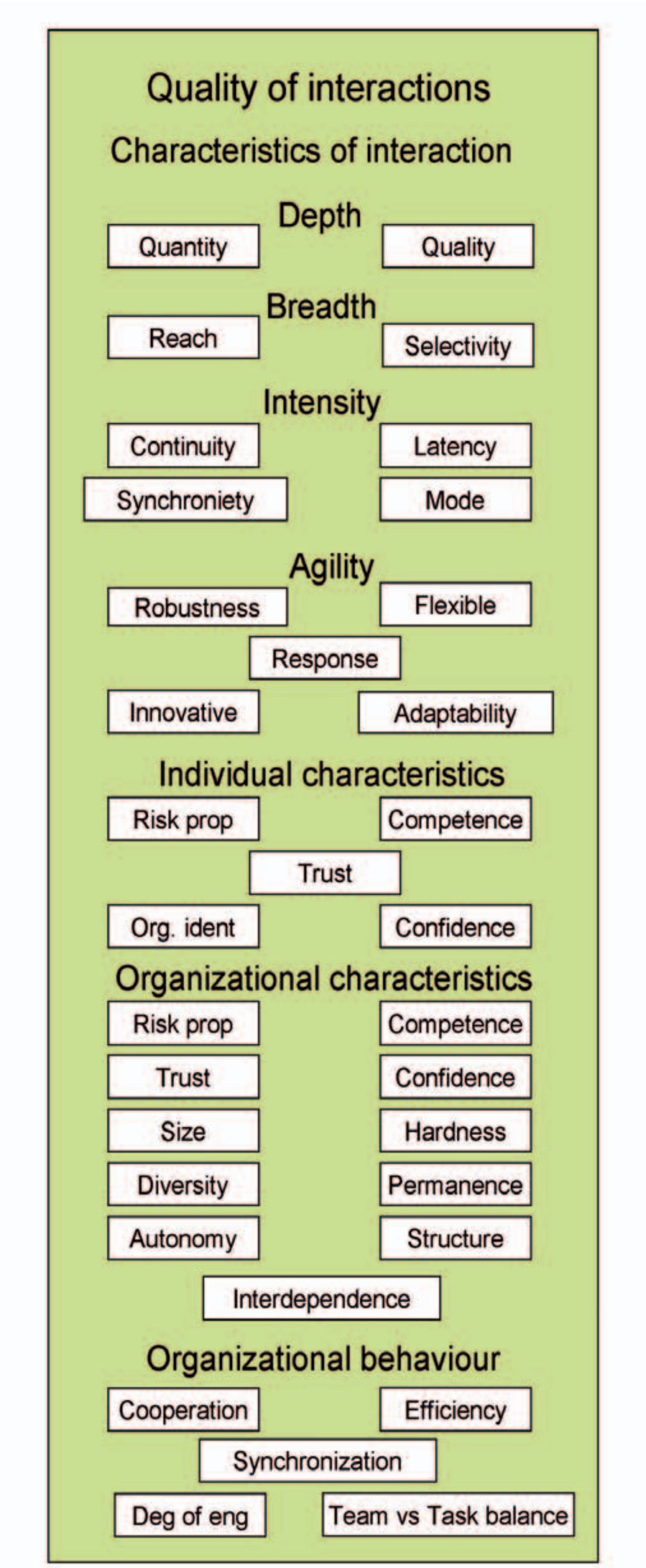


Fig 11. Quality of interactions

This view does not reflect the nature of relationships that are necessary for in-depth information sharing with numbers of external groups as would be required for NCW to be fully working in a large multinational force. Recent work in social psychology [4] has shown that these depend on the strength (strong or weak) and quality of relationships (relational or collective identity) as summarized in table 1.

Table 1
Outcomes from quality of relationships [4]

Quality of relationships \ Strength of relationships	Low	High
Collective	Fragmentation and inertia	Assimilation
Relational	Cooperative experimentation - learning	Refinement cooperation

A collective identity is strongly internally oriented and hostile to those outside the group. The RMCS cultural perspective suggests that this is true of the Army motivational pattern of building up strong internal relations, possibly at the expense of other groups [1]. A relational identity seeks to build positive relations with the outside world. Collective identity with weak relationships tends to ignore the outside world, leading to inertia and fragmentation as it becomes increasingly unable to cope with changes in the outside world. Collective identity with strong relationships leads to assimilation (ie, an aggressive take-over) of other parties that get close, which again does not lead to learning.

Relational identity with weak relationships leads to cooperative experimentation where learning will take place. Relational identity with strong relationships leads to refinement cooperation where ideas will be improved through cooperation.

A further cause of differences in interactions between different groups stems from cultural differences between nationalities. The main factors, summarized from [6] are:

- behavioural differences, eg, eye contact
- value systems, eg, power distance affects leadership style
- cognitive differences, eg, diverse reasoning styles
- factors affecting C2 performance –differences in:
  - risk and uncertainty avoidance
  - activity orientation, eg, prefer 'doing' to 'being' or vice versa

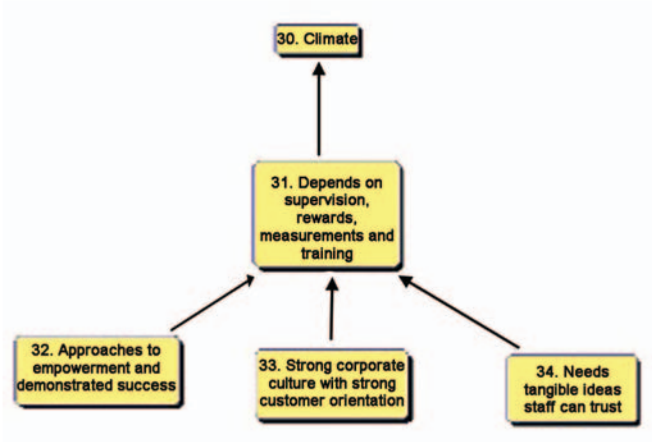


Fig 12. Factors affecting organizational climate

– dialectical reasoning, eg, Westerners tend to use debate to sharpen up a solution whereas non-Westerners may compromise and incorporate all solutions

– counter-factual reasoning, eg, far greater use of 'what-if' reasoning in Western than in Eastern cultures.

The above factors show a wide range of cultural differences between nationalities that could limit the quality of interactions. There are no clear solutions to these occurring other than being made aware that they could happen and adjusting accordingly when they do.

Aspects not covered in NCW framework

There were several social factors not included in the NCW framework that could have a potentially major impact, primarily from organizational psychology. The survey of civil digitized systems [5] indicates that organizational climate is very important in high-pressure situations, as illustrated in figure 12. In a high-pressure environment in which NEC is expected to operate, it is important to use supervision, rewards, measurement and training to ensure that motivation is maintained.

A further factor that was found to contribute to success was using business process re-engineering to maintain flexibility and control [5]. The ability to maintain control is viewed as very advantageous in a highly competitive environment. Use of process engineering may provide a further potentially useful tool in the military domain.

If any organization, NCW/NEC included, is operating in very stressful environments, Mintzberg [7] has suggested such organizations are likely to evolve in the following way:

- the more dynamic the environment, the more organic the structure (ie, it has loose relationships)
- the more complex the environment, the more decentralized the organizational structure
- the more diversified the organization's markets, the greater the propensity to split into market-based units

Table 2
Summary of social factors

NCW area	Social factors	Components of social factors
Degree of shared information	Openness	Willingness to put cards on table
	Trust	Faith
Degree of shared sense-making, shared awareness and shared understanding	Social - strength of ties	• Frequency of interaction • Extended history • Intimacy or mutual confiding
Quality of collaborative decisions	Agility	Speed of decision
	Situation awareness	see tables 4 and 5
	Project management	Demands of technology versus demands of situation
Quality of interactions	Strength of relationships	• Strong • Weak
	Quality of relationships	• Collective • Relational
	Cultural	• Behavioural differences, eg eye contact • Value systems, eg power distance affects leadership style • Cognitive differences, eg diverse reasoning styles • Factors affecting C2 performance
Other (not in NEC)	Organizational climate	Good leads to high motivation; poor leads to poor motivation
	Effect of dynamic, complex environment on organizations	• Organic structure (with loose relationships) • Decentralized • Divided into market-based units • Decentralized and differentiated work units
	Re-engineering to achieve management control	

- the greater the disparities in the environment, the greater the trend towards decentralized and differentiated work groupings.

These relationships imply that, to be successful, NCW organizations will develop into a very decentralized, differentiated organizational structure. Where such decentralization does take place, it may lead to information not being shared between different decentralized units.

Summary of social factors

A range of social factors have been identified as potentially affecting NCW, and these are summarized in table 2. There are few tools that can be readily identified for gathering metrics for most of them. The factors are qualitative and data can be gathered for most of them using interviews or questionnaires. If more in-depth data were required, rating-scale questionnaires would be likely to be useful.

The social and cultural factors identified represent a major pitfall for those developing NCW technology. In any studies of NEC/NCW systems, there should at least be informal sounding of the members of a force to check that they have good relationships and are willing to share information with the other members, and that they are not holding back owing to some cultural or social factor. Table 2 provides a useful checklist of the factors that could be having an effect.

The factors in table 2 should be reflected in the current NEC/NCW metrics work, which should also address organizational climate and the requirement for organizations operating under stressful conditions to evolve to achieve their best possible level of performance, if not currently covered.

The RMCS cultural factors do pose very major questions to those trying to develop NEC/NCW operations. The factors in table 2 do show how it may at least be possible to begin to overcome these obstacles. Table 2 should provide a useful reference source for those exercising command in a multinational force and, for their subordinates, of the main ways of building up trust in a force with different backgrounds that has to relate by a network rather than by direct physical contact.

4 CONCLUSIONS

NEC/NCW is about developing networked forces with greater shared awareness, leading to greater self-synchronization, leading to faster speed of command and improved lethality and survivability. Two perspectives have emerged in the behavioural and social NEC/NCW research: a cognitive social psychology perspective aimed at 'organizational sense-making' to derive metrics and tools for NEC/NCW, and a culturally-based perspective highlighting problems of using NEC/NCW technology with current mind sets that are based on holding on to information rather than sharing it.

The work described in this paper covered perspectives from social psychology and organizational psychology, using cognitive mapping (a soft OR technique) and an NCW framework [9] for determining metrics. The social psychology perspective is based on building up trust between groups to foster working together effectively and could address some of the cultural barriers. From organizational psychology, areas not currently covered under NEC/NCW research are organizational climate and organizational structure, focusing on how they evolve to meet the demands of a stressful environment.

The presence of such social and cultural barriers presents a major test for those interested in developing network technology, as it may be difficult to tell whether shortfalls in the network are caused by technical or social factors. It is recommended that the presence of social factors should be checked by interviews with the different parties in a force.

The trust factors described in this paper do provide commanders with potential mechanisms for building up relationships between different units in a disparate multinational force.

As a number of the social factors described are in other, non-defence environments, it would be useful to test their occurrence in realistic multinational force experiments and exercises. The measures suggested for building up trust in a force are potentially useful and their suitability should be assessed for use in operations.

5 DEFINITIONS

Table 3
Degree of shared information

Attribute	Definition
Objective measures	Measures quality in reference to criteria that are independent of the situation
Extent	Proportion of information in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share information item
Correctness	Extent to which shared information is consistent with ground truth
Consistency	Extent to which shared information is internally consistent with prior information / awareness / understanding
Currency	Age of shared information
Precision	Level of measurement detail of shared information item
Quality	Measures quality in reference to criteria that are determined by the situation
Completeness	Extent to which shared information relevant to ground truth is obtained
Accuracy	Appropriateness of precision of shared information for a particular use
Relevance	Proportion of shared information retrieved that is related to task at hand
Timeliness	Extent to which currency of shared infomation is suitable for its use

Table 4
Degree of shared sense-making: shared awareness

Attribute	Definition
Objective measures	Measures quality in reference to criteria that are independent of the situation
Extent	Proportion of awareness in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share a given awareness
Correctness	Extent to which shared awareness is consistent with ground truth
Consistency	Extent to which shared awareness is internally consistent with prior awareness
Currency	Time lag of shared awareness
Precision	Level of granularity of shared awareness
Quality	Measures quality in reference to criteria that are determined by the situation
Completeness	Extent to which relevant shared awareness is obtained
Accuracy	Appropriateness of precision of shared awareness for a particular use
Relevance	Proportion of shared awareness obtained that is related to the task at hand
Timeliness	Extent to which currency of shared awareness is suitable for its use
Uncertainty	Subjective assessment of confidence in shared awareness

Table 6
Quality of collaborative decisions (1)

Attribute	Definition
Objective measures	Measures quality in reference to criteria that are independent of the situation
Extent	Extent of force entities that reach a collaborative decision
Consistency	Extent to which decisions are in agreement across force entities within and across CoI
Currency	Time lag of decisions
Precision	Level of granularity of decisions
Fitness for use measures	Measures quality in reference to criteria that are determined by the situation
Appropriateness	Extent to which decisions are consistent with existing shared understanding command intent and shared team values
Completeness	Extent to which relevant decisions encompass the necessary: • Depth: range of actions and contingencies included • Breadth: range of force elements included • Time: range of time horizons included
Accuracy	Appropriateness of precision of decisions for a particular use
Relevance	Proportion of decisions that are important to the accomplishment of the task at hand
Timeliness	Extent to which currency of decision making is suitable to its use
Uncertainty	Inter-subjective assessment of confidence in decisions
Risk propensity	Extent of risk aversion
Mode of decision making	Type of collaborative decision making structure utilized (authoritative decision making, consensus building, majority rule, etc)

Table 5
Degree of shared sense-making: shared understanding

Attribute	Definition
Objective measures	Measures quality in reference to criteria that are independent of the situation
Extent	Proportion of understanding in common across force entities, within and across communities of interest (CoI) Proportion of force entities that share a given understanding
Correctness	Extent to which shared understanding is consistent with ground truth
Consistency	Extent to which shared understanding is internally consistent with prior understanding
Currency	Time lag of shared understanding
Precision	Level of granularity of shared understanding
Quality	Measures quality in reference to criteria that are determined by the situation
Completeness	Extent to which relevant shared understanding is obtained
Accuracy	Appropriateness of precision of shared understanding for a particular use
Relevance	Proportion of shared understanding obtained by force member that is related to the task at hand
Timeliness	Extent to which currency of shared understanding is suitable for its use
Uncertainty	Subjective assessment of confidence in shared understanding

Table 7
Quality of collaborative decisions (2)

Attribute	Definition
Agility	Degree to which force entities were robust, flexible, responsive, innovative and adaptable
Robustness	Degree to which collaborative decision is dominant across a range of situations and degradation conditions
Flexibility	Degree to which collaborative decision allows force entities to maintain flexibility (ie, incorporate multiple ways of succeeding)
Responsiveness	Degree to which collaborative decision is relevant and timely
Innovativeness	Degree to which collaborative decision reflects novel ways to perform known tasks and / or develop new ways of doing novel tasks
Adaptability	Degree to which collaborative decision facilities force entities' ability to alter the decision, decision making participants and / or decision making process and implement appropriate modifications

Acknowledgements:
The author thanks Dr Olympia Kyriakidou and Dr Panos Louvieris from the School of Management, Surrey University for their contribution [4,5], Dr David Signori, RAND, whose work provided an invaluable framework to this study [9], and Tracy Gardiner, Information Management, and other Dstl colleagues, for their support in writing this paper.

References:

1 Bradley D R, Strickland G M, Walker C R V and Woodisse R W. *Networked Enabled Capability and British command culture.* No 6 DTC Project Study Report. MA Thesis RMCS Shrivenham (June 2002).

2 Houghton P, Leedom D and Miles J. *Command Information Sense-making*. 7th International Command and Control Research and Technology (ICCRTS) Symposium Québec City, QC, Canada (16-20 September 2002).

3 Leedom D. *Shared creation of knowledge: metrics for assessing the impact of information technology on organizational sense-making*. Evidence Based Research. (September 2002).

4 Kyriakidou O. Identity orientation and networking: *Towards a conceptual framework for understanding of organizational change*. British Academy of Management, London (9-11 September 2002).

5 Louvieris P and Phillips P. *Optimization of organizational structures and processes to benefit digitization (includes survey of industry)*. University of Surrey School of Management Report (March 2002).

6 Klein H A, Pongonis A and Klein G. *Cultural factors on multinational DM*. DARPA Contract No: DAAH01-00-C-R094 (2002).

7 Mintzberg H. *The Structure of Organizations*. Prentice-Hall. (1979).

8 Eden C and Ackermann F. Chapters 2 and 3, *Rational Analysis for a Problematic World Revisited. Problem Structuring Methods for Complexity, Uncertainty and Conflict*. Eds J Rosnehead and J Mingers. Wiley. (2001).

9 Signori D. *Conceptual framework for NCW assessment,* RAND (in collaboration with Evidence Based Research). (17 October 2002).

HVR Consulting Services Ltd, Selborne House, Mill Lane, Alton, Hampshire GU34 2QJ
John.Holt@hvr-csl.co.uk

Commanding Agile Mission Groups: a speculative model

NEC Delivery Project Team[1]

Lt Col Merfyn Lloyd OBE RWF

No new weapons can be introduced without changing conditions, and every change in condition will demand a modification in the application of the principles of war.
– Major General J F C Fuller, Armoured Warfare, 1943.

The command of troops in war is an art, a free creative activity based on character, ability and powers of intellect.
–HDV 100/1, Truppenfuehrung*, 1962 (Troop leadership in the German Army).*

Abstract

Network Enabled Capability calls for a major revision of the way command is exercised in military operations. In the development of a conceptual framework for NEC, effects on command have been examined. Central to ways of improving operational effectiveness is the ability to deliver effects throughout the battlespace by the dynamic formation of agile mission groups. The command model developed requires a high level of shared awareness and command intent within and between AMGs, with an inbuilt awareness of the need to adjust to circumstances. The command management function derived meets the requirements of the high-level operating concept for agile forces, and in turn the aspirations of NEC.

INTRODUCTION

Recent work to develop a Network Enabled Capability (NEC) Conceptual Framework [1] has considered the application of the emerging concepts to military operations, first, to try to gain a better understanding of the concepts and their implications and, secondly, to find a readily recognizable and understandable way in which the concepts could be explained to a general audience. To do this, seven 'use cases' or scenario vignettes were collected from the 'capability chain' concept being developed elsewhere in the MoD, primarily in support of the Equipment Capability area's capability audit. Initial work [2] with these use cases identified how NEC might improve current processes, to do what is done now but more effectively. However, the real potential of NEC lies in its ability to allow ends to be achieved in new ways that improve the operational effectiveness of UK forces.

Central to this is the ability to deliver effects throughout the battlespace by the dynamic formation of agile mission groups (AMGs), a need recognized in both the Joint Doctrine and Concepts Centre's (JDCC) High Level Operating Concept (HLOC) [3] and the NEC conceptual framework. Thus, an important next step in considering the use cases is to consider how AMGs are to be used, how they form and how they are best commanded. In an earlier paper [4], the view was taken that a functionally orientated command structure might be more beneficial than the current environmental component structure in enabling the formation of joint tactical AMGs.

This paper builds on these ideas and those expressed in the HLOC and NEC conceptual framework to develop a model for the command of AMGs that can be applied in the use cases to identify new ways of achieving the desired outcomes.

1 The NEC Delivery Team is the core NEC project and is led by Dstl with support from QinetiQ and other industry. The project manager is Jonathan Williams.

INITIAL USE CASE DEVELOPMENT

Initial use-case work selected five capability-chain scenarios being developed primarily for capability audit purposes. Since these were all based on warfighting, two more were added to cover Peace Support Operations and Counter Terrorism. The seven are:

- urban operations –to clear and maintain a Main Supply Route (MSR) through a hostile urban area to support operations elsewhere
- biological attack –to limit the effects of a biological attack on a force preparing for an operation in order to maintain its viability for future operations
- force deployment –to deploy reinforcements and logistical support rapidly via a single joint logistics chain to sustain a small, established force
- air manoeuvre –to prepare and sustain a Forward Arming and Refuelling Point (FARP) to support a transiting force already embarked
- joint fires –to coordinate an attack using maritime, land and air assets on a withdrawing divisional-sized target to prevent its escape
- counter terrorism –to provide military support to the civil authorities to protect life
- peace support operations –to coordinate British forces under UN command, and the response of the UK government, to contain the escalation of a low level, high profile, incident so preventing further conflict –the 'strategic corporal' effect.

The methodology used in this initial assessment is described in [2]. A key element was the identification of a Military Measure of Effectiveness (MMOE), that is, the criterion by which the military commander of the operation would judge its success. For example, when considering the urban operations use case, the MMOE applied was the 'ability for convoys to transit the MSR at any time without loss', with the prime characteristics of timeliness and the size of the force required to maintain the MSR open. From this, subordinate MMOEs were derived and used to measure current capability. They were then used to measure any theoretical advantage or disadvantage that NEC might provide in conducting the same operation, and the difference between the two measures was taken as an illustration of an NEC benefit or degradation to operational capability.

The essential character of this stage of the analysis is that of seeking to improve on current processes. In the next stage, new processes are required that take advantage of information technology and allow the development of NEC as described in the capability framework [1]. These two stages can be referred to as the 'industrial age' and the 'information age' views and are shown in figure 1 as being steps along an NEC route map. In completing the industrial age analysis, the justification for potential NEC benefits was related back to the NEC themes [2]. Unsurprisingly, this showed that the key to improving current process is to enhance our ability to share information and to work collaboratively. To move beyond this, and be able to work collaboratively and synchronize effects in a truly dynamic way, information age doctrine and concepts are needed that provide the context for the conduct of information age operations.

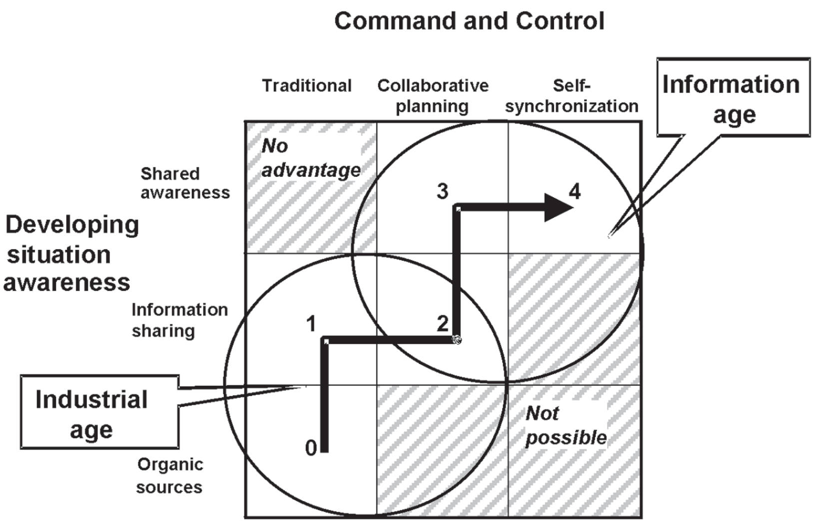


Fig 1. NEC route map [8]

2 This and similar terms are discussed later. In our interpretation, shared situational awareness has the same meaning as shared awareness.

DOCTRINAL CONSIDERATIONS

The information age concepts and doctrine that provide the context for NEC are being developed by JDCC. The basis for the high-level operating concept is:

> *'An ability to conduct effects-based operations with highly responsive, well integrated and flexible joint force elements that have assured access to and unprecedented freedom of manoeuvre within the entire battlespace. Force elements will thrive upon tactical innovation, confident that the actions that they take will be intuitively consistent with strategic and operational objectives. The dominant characteristic of the future battlespace will be freedom of joint fire and manoeuvre'.*

Key to achieving this is the need for agility, characterized by four attributes:

- responsiveness: speed of reaction (to the unexpected)
- robustness: capable of multiple missions
- flexibility: multiple paths to success (unpredictability)
- adaptability: learning and adapting (to the unexpected).

To support such operations, the command core concept expressed in the HLOC reinforces the importance of mission command in the information age to delivering optimum tempo from the creativity and initiative of well-informed subordinate commanders. This will be underpinned by a network-wide expression of command intent and shared situational awareness[2], together with an adaptive command and control (C2) process that reduces the tension between freedom of action and alignment of strategic and operational goals; in short, an agile joint force empowered to exploit and create opportunities.

HLOC also describes, within the inform core concept, the need for decision superiority generated by shared situational awareness within and between mission-orientated communities of interest based on a federated information architecture to facilitate collaborative processes within a single information domain. In developing the notion of communities of interest (or AMGs), HLOC distinguishes between dynamic communities capable of dispersed collaborative planning that form as needed, and preconfigured communities based on the need to provide a specific capability.

HLOC thus provides considerable high-level context and guidance as to how future operations are to be conducted, including the requirement for and the nature of AMGs and the way in which they might be commanded. This guidance is used to develop the command model for the information age of the use case studies.

A USE CASE EXAMPLE

The urban operations use case example is used to illustrate aspects of the discussion that follows (Figure 2).

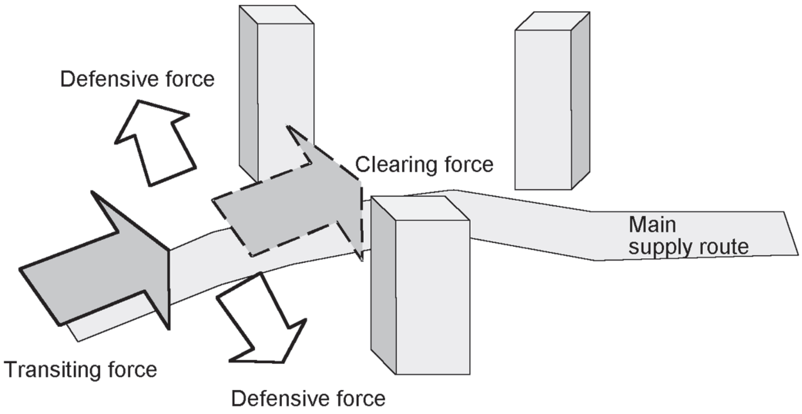


Fig 2. Urban operations use case scenario

In this industrial age view, the outline Blue Force organization is composed of an armoured brigade supported by force assets. The brigade provides a clearing force to fight and seize the route and a defensive force to consolidate and hold the route open. The transiting force is a supply convoy from Division with an escort provided by the brigade. The whole operation is supported by brigade and divisional assets including artillery, Close Air Support (CAS) and Attack Helicopter (AH) AH 64-D, in addition to ISTAR assets that include ASTOR[3] and Unmanned Aerial Vehicles (UAVs) (for example, WATCHKEEPER).

Figure 3 shows the related synchronization matrix for the major capability elements of the force. This illustrates the procedural, linear sequencing necessary to command and control the operation if all the requisite information is to be gathered and processed, plans are to be developed, orders issued, assets deployed, the enemy engaged and the operation coordinated.

Anything that can be done in the short to medium term to improve information sharing (figure 4) will benefit the overall situational awareness of the participants[4]. Nonetheless, the process will remain essentially a linear one, and the higher levels of agility sought by HLOC will not be obtained until much more dynamic information age process is in place to improve shared awareness[5].

SHARED AWARENESS AND COMMAND INTENT

"A state that exists in the cognitive domain when two or more entities are able to develop a similar awareness of a situation. The degree of similarity required (or difference tolerable) *will depend on the type and degree* of collaboration and synchronization needed" [8].

Thus, in the NEC context, shared awareness is the ability to communicate an individual's understanding to others in order that, as a group, there is some level of shared understanding[6] [1]. It incorporates the notion that the situational awareness of the individuals participating in an operation is understood in the context of each other's roles and tasks in that operation; that is, the views held by an individual are recognized and understood by everyone else in an AMG and allow each to access the detailed information he needs to prosecute his role in the battle[7].

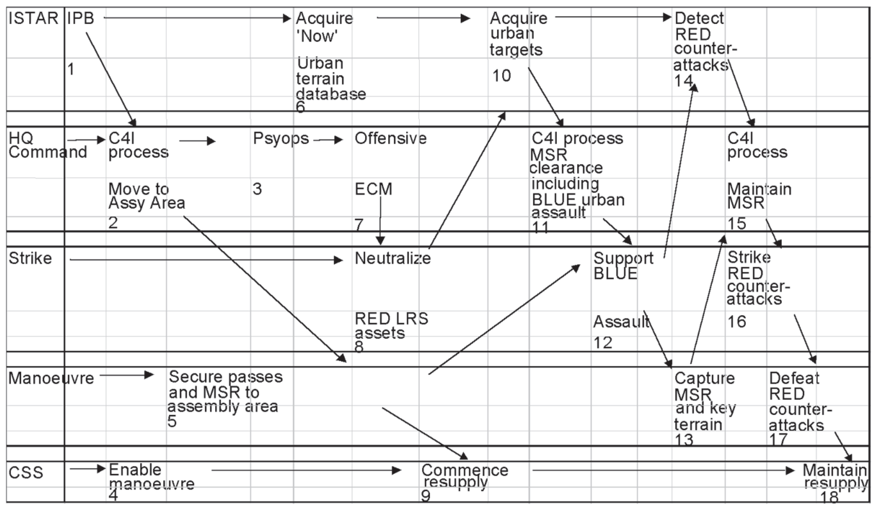


Fig 3. Industrial age synchronization matrix

3 Airborne STand Off Radar.

4 An example of such an improvement is the provision of Blue Force Tracking technology to British Forces in the Iraqi War 2003.

5 Awareness exists in the cognitive domain. It relates to a situation and, as such, is the result of a complex interaction between prior knowledge (and beliefs) and current perceptions of reality. Each individual has a unique awareness of any given military situation. Here again, professional education and training are used in an effort to ensure military personnel with the same data, information and current knowledge will achieve similar awareness [8].

6 Understanding involves having enough knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation to predict possible future patterns. Hence, situation awareness focuses on what is known about past and present situations, while understanding of a military situation focuses on what the situation is becoming (or can become) and how different actions will affect the emerging situation.

7 For example, it will provide targeting information for strike assets such as Close Air Support (CAS) and artillery, as well as the broader detailed information needed by an infantry company.

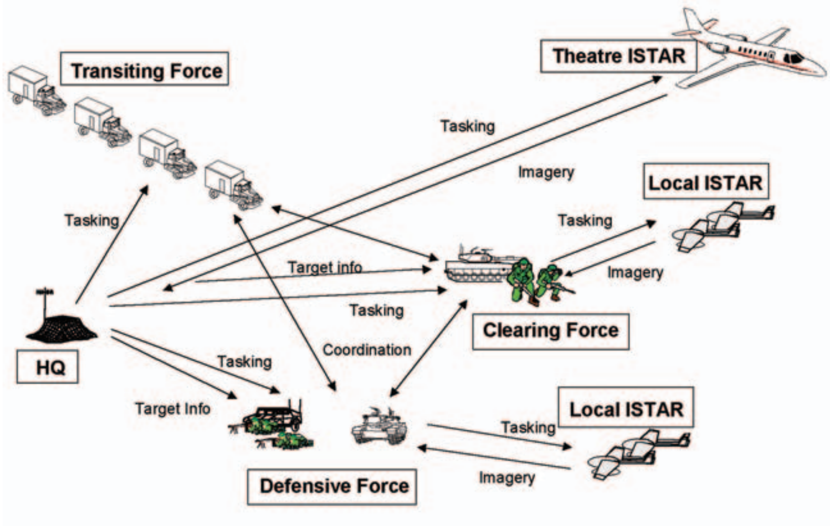


Fig 4. Information sharing

Implicitly, shared awareness incorporates the command intent pertinent to the operation so that everyone in an AMG understands not only, for example, the geo-spatial element[8] but also what it means in the context of what is trying to be achieved –that is, it brings an understanding of the future. Since shared awareness has a predictive element in respect of Red, White and Blue forces, the individual can anticipate what may happen, and be able to recognize and be ready to exploit an opportunity. Likewise, it allows him to recognize when events are not happening as expected and to make the adjustments necessary. Thus, shared awareness has two principal elements: the gathering, maintenance and presentation of information, and the development of a shared understanding of the situation based on situational awareness and command intent.

Command intent is used to describe a much richer concept of operations than the current 'commander's intent', resulting, as it does, from the integrated efforts of commanders and their staffs at different levels and from the incorporation of each commander's perspective into the whole. What emerges must become the *intent* of the whole command. Importantly, this intent will change over time; parts may remain extant throughout while other parts may change very rapidly as new situations occur. Events unfolding at the fighting level are able to influence the command intent as befits their criticality to the campaign plan. Command intent, the plan and its execution are inextricably linked: they are driven by events[9] and must be capable of responding in a precise and timely, if not an anticipatory, way if they are not to diverge at the fighting level [4].

Command intent describes the outcome a commander is expected to achieve in relation to the higher-level end-state and, as described above, it will have a MMOE attached to it so that success or otherwise can be gauged. Command intent will describe to the commander the rule-set within which he has freedom to act, setting the bounds of adaptive C2 described in HLOC, including proscribed actions in terms of effects[10]. An essential element will be the synchronization reference framework within which the higher commander synchronizes the effects he wants for achieving the desired outcome. This framework provides the commander at the lower level with reference points against which he can synchronize his own actions. This is far from being prescriptive since NEC makes this a highly dynamic, responsive and continuous process so that command intent is always relevant and opportunistic. Thus the bounds set on a commander through command intent are inherently flexible, to be tightened and loosened as needed to maintain his synchronization with other AMGs and between the components of his AMG. Command intent may also specify the creation and maintenance of pre-configured AMGs to provide specific effects as part of the higher plan.

THE DECISION-MAKING PROCESS

A commander, therefore, receives his tasking or mission as a specified outcome, together with the higher commander's MMOE and the constraints that surround it. The commander then selects the effect or effects that best achieve the desired outcome and configures AMGs to deliver these effects. In the use case example, the desired outcome is 'to maintain supply' and the primary effect is 'to capture and hold the MSR and key terrain'. The commander has two measures of the effectiveness of his plan: a comparison of desired and achieved outcomes and a comparison of planned and achieved effects. Both are important since an effect other than that planned may achieve the outcome and the commander must be able to recognize it, while conversely, delivering the planned effect may not achieve the desired outcome.

The development of the plan and its execution in terms of the desired outcome, the effects needed to meet it and the AMGs to deliver these effects, are done by a process of dynamic collaborative interworking (DCI), which brings together the planning and execution of an operation in a single interactive process. This process unites commanders and their forces at all levels and has two key elements: the ability to constantly and accurately evaluate the effects and outcomes achieved against those planned and desired; the ability to share the awareness derived from the first throughout the AMG and between AMGs rapidly so that all can maintain both their understanding of what is happening around them and their synchronicity. However, the extent to which an AMG can re-synchronize in response to external events is clearly governed by the need to achieve its outcome in accordance with the command intent. Nonetheless, if an unexpected opportunity arises to achieve that outcome in a totally different way, the

8 Such as that provided by Blue Force Tracking.

9 These events are not just a reaction to the enemy but the set of all events however and by whomsoever caused. They include, therefore, events caused by the enemy, friendly forces and third parties.

10 Comparable to the current rules of engagement.

process must be sufficiently agile to allow it. In response, the AMG may have to 'mutate' by gaining or losing components, suggesting that in exceptional circumstances it could do so several times in the course of a task.

Figure 5 attempts to capture this. The DCI process is shown in outline in the centre, and the contributions by and to shared awareness and command intent are shown around the outside. NEC makes this highly dynamic[11] by facilitating the creation of shared awareness both within and between AMGs. DCI moves away from the rigid 2-dimensional hierarchical structure of current planning and control processes to a more agile 3-dimensional model where the processes that constitute DCI are shared vertically and horizontally. These processes are those that maintain coherent command intent and shared awareness by relating outcomes to other outcomes, effects to other effects and the resources of one AMG to those of others, together with an understanding of the operational situation in time and space.

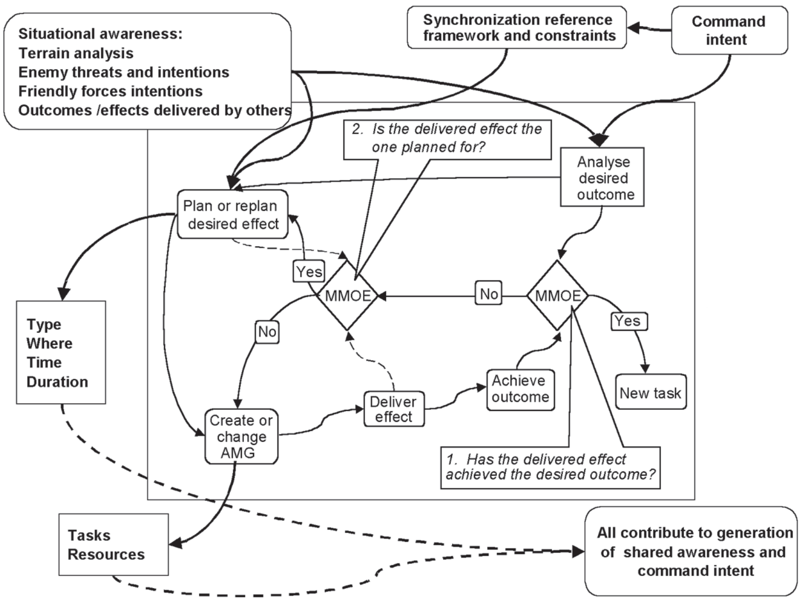


Fig 5. Dynamic collaborative interworking –outline process

The commander needs to analyse the outcome he has to achieve and its MMOE. As he was a party to its determination through the collaborative and interactive nature of DCI, he understands why it has to be achieved but needs to relate it in detail to the situation in which he must bring it about. He needs to have access to the appropriate information to do this, which must be focussed to his needs. It will provide him with the geo-spatial context, detail of the enemy threats in terms of size, location, capability and intent. Similarly, he will need to know the detail of friendly forces that affect him or could be available to him if needed and of neutral groups such as refugees. Determining the key effect and how to apply it will involve careful consideration of the outcome, the effect on the enemy he wants to achieve, the consequences of that effect on the enemy, himself, and others, as well as the effects of terrain. Here, he will be guided by the requirements of the synchronization reference framework and the constraints given in the command intent but, again, as he is party to the higher-level determinations and, in particular, the resources that are likely to be made available to him, he probably has a clear idea of what he would like to do. From this he is able to determine how this effect will be achieved and what resources he will have to use. Again, it is important to note that he is doing his planning directly and interactively with his subordinates and his staff. This is not so much planning by consensus but getting early 'situational immersion' in the operation so that problems can be resolved sooner rather than later. His direction, in the form of well-developed command intent, flows both downwards to guide the operation and upwards to add to the shared awareness of higher command.

The emphasis on developing high levels of shared awareness and richness of command intent through the DCI process means that much of the understanding currently developed through the estimate process and expressed in formal orders is already present. Minimal direction, such as that contained in the command intent, is needed, making it unnecessary to specify detailed control measures such as boundaries and coordination lines. This is not a recipe for chaos as the need to achieve specified outcomes focuses the actions of AMGs while leaving them free to exploit opportunities. The process of comparing desired and achieved outcomes means that the commander commands by exception, only intervening when he feels it necessary to do so to re-task the components under command.

Command management is the means by which these command arrangements are established and maintained. These arrangements must reflect the principles of mission command and the need to allow elements of the AMG to cooperate naturally and in a way that is related to events as they occur, especially in terms of synchronization. Command management allows the commander to create the command arrangements he requires to fight his AMG. This therefore includes information management, configuring facilities and establishing services that facilitate the smooth and timely flow of information across the battlefield [9].

STRUCTURE OF AGILE MISSION GROUPS

Earlier analysis [4] has shown that the components of the Defence Capability Framework (DCF) [7] provide a useful way of describing the capability of a force, or in this case an AMG. These capabilities are generic to every force to a greater or lesser degree and can be grouped as either core capability or enablers, as shown in table 1.

[11] Compared with current process for examples of which see [5] and [6].

Table 1
Defence capability framework

Capability	Explanation	Remarks
Command	The command and management of forces under command	Core integrating capability
Operate	The ability to fight the enemy by striking, manoeuvring or using other effects against him	Core fighting capability
Inform	The collection and processing of the information needed to conduct operations	Key operating enabler
Protect	The ability to protect the force from a wide range of hostile action and from the environment	Key operating enabler
Sustain	The ability to sustain the force throughout the operation	Key operating enabler
Project	The ability to project the force into the theatre of operations	Key deployment enabler
Prepare	The ability to prepare for operations	Key deployment enabler

'Command' is the core capability that brings all the others together and gives the force its purpose. 'Operate' is divided into strike, manoeuvre and 'other effects' such as information and psychological operations and command of Special Forces. 'Prepare' and 'Project' are considered to be high-level enablers that affect the deployment of the force into theatre. From this, a generic AMG structure can be described, consisting of elements of strike, manoeuvre and other effects enabled by the inform, protect and sustain functions, as shown in figure 6.

The implication of this is that there is a higher-level functional command structure, rather than the current environmental component structure, consisting of commanders for each functional area, such as Commander Manoeuvre, Commander Strike, Commander Other Effects, Commander Protect, Commander Inform and Commander Sustain. Each of these commanders is *de facto* a joint commander responsible for the command and coordination of assets from all environments that contribute to that function and for their contribution to and support of AMGs whether their own or others. Thus, in the use case example, Commander Inform is responsible for supplying the AMG undertaking the operation with the information it needs to undertake that operation. To do so, he may deploy assets, such as ASTOR and WATCHKEEPER, specifically to gain particular information to add to the information he has or is receiving from other sources. He does not supply raw data, unless in a very specific context, but a complete product to the AMG commander that is coherent with other AMGs. In another case, Commander Manoeuvre may be required to provide close-combat assets to Commander Protect for rear area protection or to Commander Sustain as part of one of his AMGs. This need to resource tasks

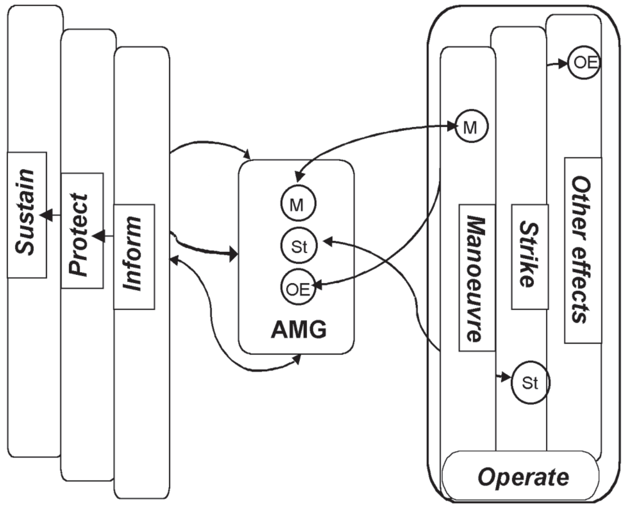


Fig 6. Generic structure of AMGs

based on outcomes is again done within DCI as an interactive process between commanders.

The AMG structure shown in figure 6 has elements contributed from the functional commanders either as core capabilities to carry out its task or as key operating enablers that support that task[12]. Some of theses core capabilities will be transient in their membership of the AMG, others more enduring; there is no hardwired ownership[13]. In the use case example, one AMG may have infantry and armour as enduring members because they are needed throughout to achieve the outcome, whereas the strike elements, such as artillery, CAS and AH, may be transient and so able to support other AMGs. This flexibility is sought-after today but only becomes possible in the context of shared awareness enabled by NEC.

COMMAND STRUCTURE

However high the quality of the interactions provided by DCI, the AMG commander will still need to consider the resources and information he requires to make the best decision –for example, he will still have information requirements. While there may be disadvantages from a human factors perspective, NEC provides the means to create virtual command structures through collaborative working. This does not mean that the enabling functions become impersonal providers on a 'take it or leave it' basis. On the contrary, if the commander's needs are to be met and the AMG to retain its flexibility, the links

[12] AMG commander is really only interested in their products and not the mechanics of how they are obtained or delivered. Thus, in the use case example, the commander is able to assume that, because his protection is 'enabled', his air defence and rear area security are assured or at least guaranteed to a given level, while he might be directed as part of the protection measures for himself, or because it supports another AMG's task elsewhere, to implement certain restrictions or take certain actions such as not to use target-locating radars or laser markers for a given period. Similarly, in terms of sustainment, he is not concerned as to how fuel and other supplies reach him so long as they are of the correct nature, on time, in the right place and in the right quantity.

[13] The cost of ownership to the AMG commander is removed while still retaining the guarantee of effect.

must be strong and personal through the insertion of a 'virtual' staff officer into the AMG command structure, indicated in figure 7 by the broken line. This virtual staff officer has access to the full capability of his functional area and is able to tailor his support to meet the purpose of the AMG[14]. He is integral to the AMG commander's decision-making process and is responsible to the commander for the delivery of his part in the operation. In the use case example, the AMG commander has a virtual *inform* staff officer who is his link into the inform community. This officer is a member of his staff and is responsible for the delivery of the information the commander needs as and when required. The added advantage is that he is also part of the inform community, and has full access to information that could benefit the AMG commander. Importantly, this is a two-way process and he is also responsible for ensuring that the information generated in the AMG as the operation unfolds, such as the detail captured by weapon systems and FIST[15]-equipped soldiers, goes back into the inform process to improve situational awareness.

Application of the command model described above to the use cases is the next step and remains to be carried out in detail. This will consist of the generation of command intent and careful consideration of the full nature of shared awareness. A detailed expansion of the DCI process is needed to support effects-based planning, synchronized execution and the creation of AMGs. A detailed understanding of the information needs that support it and the implications for information management is essential if full information access is not to result in an information flood. These considerations, together with the infrastructure and the services required, will be addressed by MoD-sponsored studies.

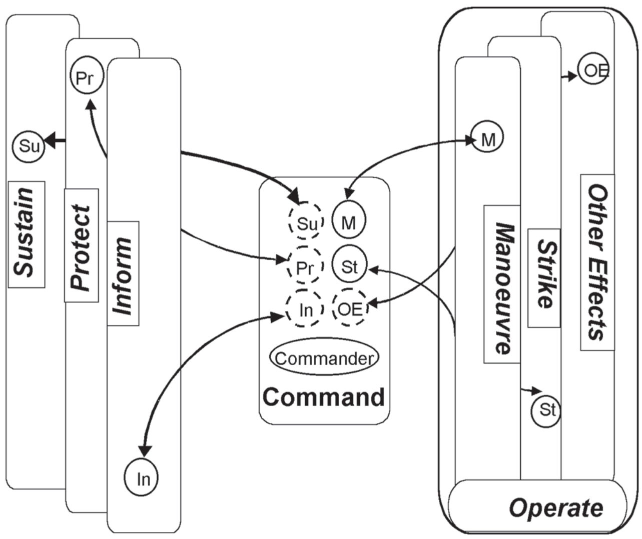


Fig 7. Virtual command structure

[14] It has the added advantage of reducing the physical size of the AMG command post.

[15] Future Integrated Soldier Technology, the UK equivalent to the US Land Warrior programme.

An interim high level but more detailed version of the model will be produced in late 2003 to allow initial gaming of the use cases to take place with the aim of identifying advantages and disadvantages associated with NEC and the metrics to support them. This will in turn suggest areas for experimentation and further study.

SUMMARY

The command model developed in this paper is based on a capability command structure derived from the components of the DCF. It requires the generation of a high level of shared awareness and command intent within and between AMGs that provides the direction, context and resourcing of an AMG. This is achieved through the DCI process that enables the commander to set tasks and measure their effectiveness by comparing desired with achieved outcomes. The AMG commander is supported by a staff with which he works interactively to plan and execute his task. Some members of his staff will be virtual, particularly those from the enabling functions of inform, protect and sustain. The command management function allows him to establish the command arrangements needed to support this, allowing him to take swift remedial action to change the effects being delivered, if necessary changing the composition of the AMG to do so. This way of command meets the HLOC requirements for agile forces and the aspirations of NEC.

Glossary

AMG	Agile Mission Group
CAS	Close Air Support
DCF	Defence Capability Framework
DCI	Dynamic Collaborative Interworking
FARP	Forward Arming and Refuelling Point
HLOC	High Level Operating Concept
JDCC	Joint Doctrine and Concepts Centre
MMOE	Military Measure Of Effectiveness
MSR	Main Supply Route

References

1 NEC Outline Concept: Part 2 –Conceptual Framework, Dstl/IMD/SOS/500/2 Issue 2.0 (2 May 2003).

2 NEC Outline Concept: Part 5 –Military Operations, Dstl/IMD/SOS/500/2 Issue 2.0 (2 May 2003).

3 The UK Joint High Level Operational Concept (HLOC), JDCC/7/11/7/1 (23 Mar 2003).

4 Lt Col M A Lloyd OBE. *Command considerations for UK network enabled forces –a speculative view .* Dstl, UK. Published by CCRP in the proceedings of the 7th ICCRTS Conference, Ottawa *http://www.dodccrp.org/Activities/Symposia/7thICCRTS/fore.htm* (September 2002).

5 (British) Army Field Manual Volume 1 Part 8. Command and Staff Procedures Issue 1.4, Chapter 5 'Decision Making'. (December 2002)

6 (British Army) All Arms Tactical Aide Memoir. Issue 4, January 2002. Section 1 'Battle Planning –The Combat Estimate Process'.

7 Joint Vision 2015, D/JDCC/7/11/1 (30 May 2001).

8 Adapted from figure 76 of CCRP Publication *Understanding information age warfare,* by Alberts D S, Gartska J J, Hayes R E and Signori D A (August 2001).

9 Markham G and Duncan H. *Development of a Battlegroup model and use cases* QinetiQ (May 2003).

Dstl Portsdown West, Portsdown Hill Road, Fareham, Hants PO17 6AD
jpwilliams@mail.dstl.gov.uk

Can Network Enabled Capability be delivered?

NEC Delivery Project Team [1]

Richard Ellis
Stratum Management Ltd

Abstract
This paper explores issues related to delivering the necessary equipment capability to meet the UK's aspirations for Network Enabled Capability. We highlight the need for coordinating developments across the MoD, mechanisms for managing the technical and programme coherence between a wide range of acquisition projects, and the need to manage and anticipate changes in requirements and in technology. We suggest that a more coherent programme management approach is required to equipment capability acquisition to provide a wider view of coordinated programmes of activity and to allow intervention in acquisition projects to achieve higher-level programme goals. This approach would enable equipment capability to be managed in the context of coherent and coordinated co-evolution of capability.

INTRODUCTION

From an acquisition viewpoint, NEC is an initiative to *improve the capability and effectiveness of UK forces through the better exploitation of information*. In early studies into NEC, nine core themes were defined and endorsed [1]. Eight of these are directly related to desired developments in capability; the ninth theme***, inclusive flexible acquisition***, differs by concentrating on *how* the capability will be delivered. It is defined as:

> *A coordinating process across MoD, other government departments and industry that promotes the rapid insertion of new technologies, facilitates coherence between acquisition programmes and provides an incremental approach to delivering 'net-ready platforms'.*

This definition highlights ***coordination and coherence*** and ***managing change***, the principal aspirations and challenges for NEC acquisition. It could be argued that these are not so different from the established aspirations of the MoD's acquisition system. Indeed, it is acknowledged that there are few challenges in acquiring NEC (or indeed in NEC itself) that are completely new, and that many of the problems will be familiar to any experienced or enlightened project manager. However, it is argued that the scope and depth of NEC bring many familiar problems into sharp focus, and make their effective resolution essential if the overall aspirations of NEC are to be realized. It is also noted that, though many of the challenges explored in this article are familiar, the MoD has not always been effective in resolving them.

ACQUISITION PROGRAMME COORDINATION

The aspirations of NEC will not be met by a single project or a small number of projects; success will be critically dependent on the delivery of capability through coordinated activities across many acquisition projects, delivered by a wide range of IPTs. Although core information technology and C2 projects will form the focus of equipment required to deliver NEC, most acquisition projects could be affected by the implications of adopting a shared information approach and presenting a coherent representation to all operators.

The wide range of projects involved in NEC, and their complex interrelationships, create an unprecedented problem in maintaining coherence. Each of the projects will have its own independent (and in some cases conflicting) timescales, requirements, challenges, funding and priorities. In many cases, projects will have different customers in MoD and principal support from different military domains, or different operational or non-operational organizations. Within this diverse mix, it will be necessary to manage a coherent development of capability, and the synchronized and coordinated delivery of services and systems.

PROJECT INTERRELATIONSHIPS AND INTER-DEPENDENCE

The interrelationships between projects take a number of forms, each with its own challenges:

Interoperability constraints

Interoperating systems need to share compatible interface standards and a shared definition (or *ontology*[2]) of information to be transferred. Interoperability constraints of this type will be familiar to many military project managers but have not always been well handled.

[1] The NEC Delivery Team are led by Dstl with support from QinetiQ and other industry.

[2] *Ontology* is used in this context to indicate a definition of the objects that can be communicated and their interrelationships. A rich shared ontology, which goes beyond traditional data models, will be required if NEC systems are to share and process concepts such as intent, understanding and plans successfully.

Provision of essential components and services by one project to another

If the expected benefits of coherence and economies of scale are to be achieved, it may be expected that more acquisition projects will have to rely on others to provide essential system components (such as software applications or toolsets) or services (such as information transfer services). Problems caused by this type of interdependency will not cease on initial supply of the component, as the delivered systems and the component itself will have to be supported and updated through life.

Timescale interdependencies

Each project will have its own timetable for the delivery of its principal capability. History suggests that many of these timetables will change during the development of the system owing to delays caused by changed funding priorities, unexpected difficulties in developing the capability, or for other reasons. Where projects are self-contained, these slippages may be little more than an inconvenience. However, where there are complex interdependencies, a small delay in one project can seriously delay other programmes. Timescale interdependencies are not limited to in-service dates: for example, decisions relating to one project will be constrained by decisions made in others, and decision-making delays may have knock-on effects in other projects.

PROGRAMME RESILIENCE

Another aspect of acquisition management related to project interdependence is that of overall programme resilience. Significant risk can be unintentionally generated when the overall programme is sensitive to failure or delay in one or more specific projects. These might be key infrastructure elements, providing essential communication or interfacing services, or specific capabilities, without which other capabilities cannot function efficiently. This can lead to disproportionate risk being placed on the success or failure of individual projects, and hence on the delivery of the overall capability required. If this risk is to be avoided, it is necessary to:

- fully understand the interdependencies between elements of a programme (including the non-equipment elements)
- develop the programme such that critical points of failure are avoided or minimized through programme-level risk management, and by planning for alternative capabilities and contingencies to be brought into play by failure of a critical project.

It is appreciated that de-risking programmes in this way is not without its costs, as it can be argued that redundant capacity is being developed and funded. However, this additional cost must be seen and assessed in the context of overall programme risk, and will often be an acceptable price to pay for the lower risk achieved.

INCREMENTAL ACQUISITION

Incremental acquisition of capability will be a key element in the delivery of NEC. The increments in capability will, however, need to be coordinated across many projects (IPTs) if overall capability is to be advanced. This approach goes beyond incremental acquisition as currently practised in MoD, and requires an overall capability management structure that can coordinate requirements, new programmes and incremental developments across many IPTs. This might, in some cases, involve intervention in existing projects to ensure that all aspects of a new capability are delivered coherently. This ability to intervene will be essential if the required flexibility and agility in acquisition are to be achieved, to meet unexpected changes in requirements and to capitalize on new developments in technology as they arise.

COORDINATION ACROSS ALL LINES OF DEVELOPMENT

A key to NEC, and perhaps one that distinguishes it from previous initiatives, is that its scope is wider than developing and fielding better systems for distributing and processing information. As indicated by the themes [1], its scope spans developments across all the MoD's lines of development[3] and, if NEC is to work, it will be necessary to manage the co-evolution of capability across a wide range of diverse organizations. Failure in achieving this will lead to a mismatch in expectations or developments in one line of development that might render advances in the others ineffective. For example, a command and control system to support a headquarters must match the force structure in which it is to be used, and the procedures and tactics that the operational commander expects to use. The users (and maintainers) of the system must have been trained in its use, and the system will need to be suitably supported. This coherent development, across diverse organizations, will only be achieved by close inter-involvement across all lines of development. For NEC, which includes the concept of effects-based operations, combining military force with diplomatic and financial levers of power, this coordination may have to extend beyond traditional MoD organizations, and embrace coherence with developments in other government departments.

It may be expected that a greater emphasis on the use of experimentation will provide a key element of support for this co-development. Experimentation, throughout the (iterative) development of systems, involving users and concept developers, can inform the evolution of system requirements and will ensure that all parties know where others are going. This will, in turn, allow discrepancies in direction or pace to be identified and resolved. However,

3 The MoD's lines of development, as defined by the Command and Battlespace Management (CBM) Management Board, are: [force] structure and processes, concepts and doctrine, equipment capability, personnel, training and sustainment. It is recognized that there are other definitions used by different parts of the MoD but the differences are not significant for the purposes of this article.

despite the advantages that experimentation might offer, the challenge involved in achieving the required coherence across the lines of development is not to be underestimated, representing as it does a challenge to existing authority structures and independence of activity within MoD.

MANAGING CHANGE

A key to the successful acquisition of NEC will be the management of change. The timescales for military systems are long. During the typical life of a system (and even during a typical 5-year plus development period of a major project) there will be many changes that will have a significant impact on the project. These are likely to include changes in:

- **Technology.** Information technology changes beyond recognition within ten years. New technologies appear and become commonplace in the workplace and in the home, and there is a valid desire to see them exploited in the battlespace. Technologies seen as a sound basis for systems disappear, and their support disappears with them. Examples of rapid change include the facts that HTML, the core language of the internet and intranets, is only 12 years old, and Java has yet to reach its seventh birthday. Some of these changes (such as the ongoing increases in computing power delivered by processors and the attendant reduction in cost/power ratios) can be predicted with some confidence and exploited, but significant unpredictable change can still be expected.

- **Requirements.** Requirements change continually, driven by changes in doctrine, operational policy and national stance. Two years ago, few would have predicted the new focus on homeland defence and anti-terrorism operations that we are now seeing; the Berlin Wall came down only 13 years ago, heralding a fundamental change in global military requirements. It is impossible to predict the equivalent changes that might take place in the coming decade.

- **Interoperability drivers.** No country has complete control of the standards and protocols that will be required to operate with others. While there are some *de facto* and defined and agreed standards, these evolve as new applications develop and historical standards are overtaken by new capability demands.

- **Commercial practice.** The commercial world is evolving new ways of managing developments, as demonstrated by the growth of outsourcing and service-based industries, and the shift towards Private Finance Initiative solutions for many government acquisitions. The way in which the MoD conducts the acquisition and support of equipment has already adopted some of these approaches and will continue to evolve in response to changing acquisition policy and best working practice in government and industry.

- **Undertaking NEC**. In addition to requirements' changes brought about by shifts in the politico-military environment, it may be expected that, as we adopt new systems and new ways of working, we shall uncover and develop better ways of conducting military operations. These will bring new requirements not previously considered. It may also be expected that undertaking the delivery of NEC will stimulate the development of innovative acquisition approaches.

To deliver NEC, it will be necessary to ensure flexibility and agility both in the systems that we acquire and in MoD's own management structures and procedures.

FINANCIAL ISSUES

Cost prediction

In many core NEC-related acquisitions, it will be impossible to accurately predict the true whole-life cost of providing a specified capability. Even if the requirements for a system remain unchanged, the pace of change in technology and the paucity of accurate cost models to predict the through-life costs of complex systems based on commercial components will foster uncertainty. This situation will be exacerbated by the interrelated nature of many NEC capabilities, and minor changes in one area may have a significant impact on the cost/capability calculations in another.

Coupled with this difficulty in predicting costs is the challenge of demonstrating the operational improvements that will be generated by NEC-related investments. If NEC is to be a success, there will be a need to support business cases with valid and supportable evidence that the enhancements of equipment capability will improve operational effectiveness and that they represent value for money. Given that the overall NEC capability will be generated by a large number of individual acquisitions and incremental upgrades, and that some spending will be necessary to provide infrastructure with no direct tangible benefit, providing this evidence will not be simple.

PROTECTION OF INTEGRATION REQUIREMENTS

In some cases, equipment/system requirements include functionality to ensure the generation and fielding of a coherent, robust, interoperable system of systems, rather than meeting the project's own core operational requirements. For example, there may be a requirement for a sensor platform to be able to translate and forward messages to other units, acting as a node in an overall network, even though this is not central to the platform's main mission. There is a natural tendency for such requirements to be given a lower priority and so to be discarded in cost/capability trade-off activities, as the Integrated Project Team Leader (IPTL) may not see them as core project capabilities. A system will be needed to ensure that NEC-related capability requirements are protected, and that the funding allocated to them is spent appropriately.

COST OF ROBUST AND ADAPTABLE SYSTEMS

A further issue will be the cost of acquiring capability that will be robust to changes to requirement and technology. A flexible, robust, adaptable solution will often initially cost more to develop and maintain than a brittle design precisely matched to initial assumptions and requirements. However, a flexible solution will cost less in the longer term, when the cost of absorbing new requirements and capitalizing on changes in technology is considered. This means that a hard choice will have to be made regarding the initial operating capability of a system. If it is to be robust and able to provide a sound basis for future support, it will either be less capable than a precisely matched solution or it will cost more. This message is often a hard one to accept but continued insistence on producing the best solution today, without considering tomorrow, will lead to lower cost-effectiveness in the long term.

CAPABILITY PROGRAMME MANAGEMENT

These challenges imply the need for a comprehensive and responsive capability programme management approach[4]. While Smart Acquisition and the Acquisition Management System [3] provide comprehensive guidance and support for managing projects at the IPT level, MoD currently lacks a coherent formal mechanism for carrying out programme-level capability management.

A programme management approach would allow all lines of development, including equipment capability, to be considered and coordinated, thus promoting their co-evolution to ensure delivery of the capabilities envisaged by NEC. Supported by a clear and current representation of the interdependencies of the projects underway and planned, it would allow the development of an overall delivery plan, coordinating projects to deliver specific programmes. A higher-level structured view of the programmes to be delivered would provide a better understanding of the issues and challenges to be faced, and would support the management of change throughout the acquisition domain (including changes to specific programmes and the greater challenge of changes required in culture and organization).

In developing such a management system, a balance will need to be struck between the independence of IPTLs in the acquisition of their projects and the needs of the overall programme(s) (such as ability of the authorities to intervene to impose a new requirement, or to force an IPTL to follow a course that is more likely to lead to a coherent overall system, even if it is to the detriment of the individual acquisition). This will be anathema to many IPTLs, for whom fixed requirements, firm prices and the responsibility to solve the problem and manage risks in the most cost-effective manner free of outside interference, are seen as basic tenets of good management and systems engineering. However, it is considered that some move in the direction of project requirement and funding flexibility will be required if a coherent capability is to be delivered. Of course, such changes could not be imposed without some consideration of cost, and changes in funding profiles would have to be included in the management of these new requirements.

Related to this issue is the development of incentives that would allow different IPTs (including their industry partners) to pursue shared goals, and so deliver an overall programme of capability, rather than just individual projects. MoD currently lacks the ability to offer such incentives, and this can lead to insularity within individual IPTs as they strive to meet the often challenging specific requirements that have been given to them. Without the incentive to trade off specific requirements between IPTs to deliver overall programme aims, it will be difficult to persuade IPTLs to support overall-capability programme objectives.

[4] In this context, the term *programme management* relates to a "*framework for implementing business strategies and initiatives through the coordinated management of a portfolio of projects to achieve benefits that are of strategic importance.*" A *project*, in contrast, is considered to be "*a unique set of coordinated activities, with definite starting and finishing points, undertaken by an individual or team to meet specific objectives within defined time, cost and performance parameters.*" These definitions are drawn from the Office of Government Commerce Successful Delivery Toolkit [2]. In this context, most IPTs could be considered to be managing projects.

SUMMARY AND WAY AHEAD

NEC raises several issues of equipment acquisition, some of which have been outlined and explored in this article. While few of these issues are new, NEC places greater importance than hitherto on their effective resolution. The most significant issues relate to maintaining the coherent development of capability across MoD (and beyond) and to managing change in equipment capability acquisition through coordinated incremental development. The resolution of these issues will require a greater emphasis on programme management for capability development and delivery, to augment the successful project management approaches currently used by MoD.

References

1 MoD Capability Manager (Information Superiority), *Network Enabled Capability - Next Steps* (28 October 2002).

2 Office of Government Commerce, *Successful Delivery Toolkit Version 3.9* (http://www.ogc.gov.uk/sdtoolkit/index.html) (April 2003).

3 *The Acquisition Handbook, A Guide to achieving 'Faster, Cheaper, Better"*. Edition 4 (January 2002).

Dstl Portsdown West, Portsdown Hill Road, Fareham, Hants PO17 6AD
rkellis@dstl.gov.uk

The impact of Network Enabled Capability on the ISTAR system performance envelope

Stuart Eves
Information Management Department, Dstl

Abstract
Implementing network enabled capability will have implications for UK ISTAR. Four drivers for providing multiple sensor coverage are identified: cueing, fusion, rules of engagement and redundancy. These lead to a requirement for elements of multiple ISTAR coverage to be collocated, contemporaneous *and* comparable. *Four drivers on the overall ISTAR performance envelope are: evolution of UK capability, evolution of the ISTAR mix, foreign capability and contingency. To deliver this increase in network-enabled ISTAR capability, it is essential that sensor systems be developed collaboratively, not in isolation. Efficient use of enhanced network enabled capability will depend crucially on an effective collection, coordination and information requirements management process that takes due account of the detection probabilities for the various sensors against different targets. Biological analogues can provide guidance on the appropriate number of sensors to use.*

INTRODUCTION

One of the earliest US presentations on NEC included an illustration of an enemy cruise missile in flight being simultaneously 'observed' by a mix of surface-based, air-breathing and satellite surveillance assets, as might be illustrated, for example, by figure 1. To understand whether such a concept makes sense for the UK, it is necessary to examine the principal drivers on the ISTAR performance envelope, and translate them into principles for the design of a 'system of systems'.

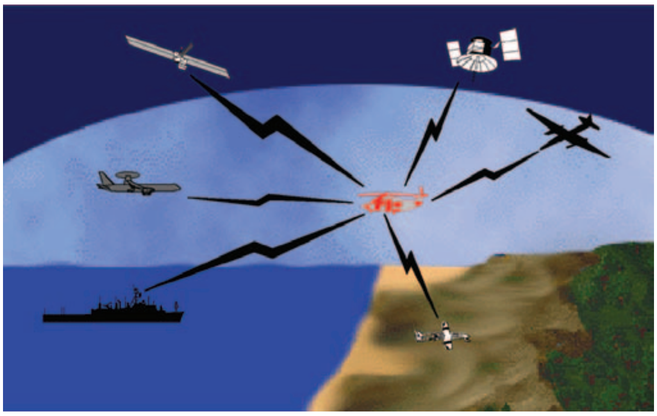


Fig 1. Network enabled surveillance

Questions that arise from such a scenario include:

1 Can the UK afford such a wealth of sensors?

2 Do all the assets brought to bear on the target have appropriate detection probabilities?

3 What is going on elsewhere in the scenario if all the ISTAR collection capability is focused on this particular target?

4 Where will the data from these sensors be fused, and do the communications links exist to transfer the data to that location in an appropriate timeframe?

5 Will analysts be swamped by the data from this number of sensors?

6 Is there an optimum number of sensors to use?

The first step to answering these questions is to develop a method for characterizing the ISTAR performance envelope.

CHARACTERIZING THE ISTAR PERFORMANCE ENVELOPE

Doing this is far from straightforward. There are, however, three high-level metrics that are commonly used to define the performance of a sensor system:

- the size of its field of regard
- the timeliness with which it provides data
- the quality (or resolution) of the information supplied, including some sense of the geolocation accuracy of the data.

These performance metrics will be used in this discussion.

PERFORMANCE DRIVERS FOR NETWORK-ENABLED ISTAR

Some significant drivers for the performance of a network-enabled ISTAR system of systems are as follows.

Cueing

The trade-off between the three principal metrics listed above means that a single sensor is often unable to meet all the desired performance values simultaneously –for example, a sensor with a large field of regard and good timeliness may lack the high quality required for certain tasks. As a result, one sensor may cue another to meet an information requirement.

To illustrate this point, NATO recognizes four general categories of task in exploiting imagery:

Detection	('There's something there')
Recognition	('The something is a tank')
Identification	('The something is an enemy tank')
Technical analysis	('The something is an enemy tank with a barrel diameter of ….')

An ISTAR system-of-systems may well involve wide-area sensors capable of, say, detecting targets, which would cue more acute sensors with narrower fields of regard, which in turn would deliver recognition and identification. For this cueing process to be efficient, it is axiomatic that the fields of view of the two sensors must coincide at some point. Simultaneous observation is not absolutely required in all cases but, since the value of information derived from a sensor is a function of time, the overall performance of the system will be greatly enhanced if the interval between successive observations is small. This is particularly the case for mobile targets, where the value of the cueing information has the potential to degrade very rapidly to the point where, later, the new target location may no longer lie within the field of view of the cued sensor, and the cueing process starts to break down completely.

Fusion

UK forces are called upon to operate in an environment in which camouflage, concealment and deception are an increasingly common asymmetric response to an ISTAR deployment. The fusion of data from several collection sources as part of an NEC is seen as a primary means of countering this threat, since creating decoys that are convincing to a number of different sensors is a more challenging task than deceiving a single one.

There are two strong drivers for requiring this collection to be as contemporaneous as possible. As with cueing, the first driver is related to the uncertainty that arises as a result of the time interval between collections (for example, does the object in this image correspond to that SIGINT contact half-an-hour ago?). This issue is particularly acute if the enemy is using deception techniques, since the two sensors may yield apparently conflicting evidence. In such a situation, there may even be value in having data from a third remote sensor (other than the human eye) to resolve the issue, a 'majority-voting' approach often adopted in safety-critical computer systems.

The second driver is related to the tempo of operations, which is a central concept for future military operations. One might assess the value of the ISTAR 'system-of-systems' in terms of the number of correct decisions made. A more robust metric, however, is the number of correct decisions **per hour**. The advantage of an NEC in countering enemy attempts at deception may be compromised if the decision-making process is slowed significantly as commanders wait for a second data collection to fuse with the first. For a fusion system to yield more correct decisions per hour, the percentage improvement in the accuracy of the decisions must outweigh the percentage increase in the decision-making time. It is left as an exercise for the reader to demonstrate that a junior officer flipping a coin once every four seconds (a system potentially capable of generating about 450 correct decisions an hour) delivers less value for money than investing in a network enabled ISTAR capability!

Rules of engagement

There has recently been an increasing emphasis on the rules of engagement for weapon systems. In general, for release authority to be granted, it is typically mandatory to have ISTAR data from at least two sources to provide target confirmation and to allay concerns about collateral damage. With the increasing use of stand-off precision guided munitions, it is unreasonable to assume that the weapon operator's eyes will provide an adequate second source. In such a case, a network-enabled ISTAR capability is indispensable.

Redundancy / robustness

For many ISTAR systems, particularly manned platforms, the concept of operations involves a stand-off range. This is a recognition of the fact that, as part of the drive for information superiority in time of war, ISTAR sensors become primary targets for offensive enemy action. Individual military systems must be designed with some inherent robustness against enemy countermeasures, but an NEC potentially offers an alternative form of redundancy through its diversity of sensor systems. Clearly, though, redundancy comes at a price, and it will be critical for the UK to determine how much ISTAR it can afford.

In a network-enabled scenario, in which multiple sensors are brought to bear on a given target, the drivers listed above indicate that sensor data should ideally be ***collocated, contemporaneous*** and ***comparable*** (in the sense that targets of interest may be unambiguously correlated between sensors).

EVOLUTION OF THE NETWORK-ENABLED ISTAR PERFORMANCE ENVELOPE

The above drivers potentially apply to the UK's existing ISTAR capability. However, in designing systems as part of a future NEC, it is important to recognize that there are a number of drivers that will cause the overall ISTAR performance envelope to change with time. Amongst these are:

Evolution of UK capability

The introduction of new weapon systems is an obvious driver for a network-enabled ISTAR capability. Long-range precision guided weapons are a good example, since they potentially require the range or area coverage of the ISTAR system to be greater. Moreover, for the terminal engagement phase, high accuracies are generally required, and this places stringent demands on the accuracy and comparability of data sets. Overlying this is a high-level manoeuvre-warfare requirement to increase the tempo of operations and shorten the decision-making cycle to enable smaller, more mobile force units to be targeted.

Evolution of the ISTAR mix

A desire to occupy the surveillance 'high ground', and an increasing reluctance to place surveillance assets and personnel at risk, mean that the future ISTAR system of systems is likely to include a greater proportion of high-altitude UAV and space-based sensors than it does at present. The effect of this change will be to improve the area coverage and timeliness of the ISTAR capability, at the potential expense of the very highest resolution data.

Foreign capability

A consequence of the high-level mandate for information superiority is that the ISTAR performance envelope must expand to provide a capability edge for UK forces. In the space-systems area, for example, the Russian Arcon satellite potentially provides greater temporal availability than Western assets, and the Helios 2/Essaim IMINT/SIGINT system planned by the French is an interesting step towards a network enabled capability.

In addition to out-performing foreign ISTAR systems, the UK's ISTAR system will also be influenced by the threat envelope of foreign weapon systems. From a defensive perspective, the NEC must enable UK forces to detect and identify enemy weapon systems at ever longer ranges. In some instances, these foreign weapon systems will have a direct impact upon the ISTAR capability itself: long-range surface to air missiles will dictate the stand-off ranges for airborne surveillance assets, for example.

Contingency

In designing the next generation of ISTAR systems, it is essential to include some degree of contingency. In part, this is to allow for the development of more sophisticated weapon systems that will be able to exploit the data provided. (In an ideal world, weapon systems and ISTAR systems would evolve in parallel. In practice, there are historical and financial reasons why the ISTAR and weapon capability increments are, and will continue to be, out of phase.) Moreover, any rigorous scientific process should make allowance for errors, and hence some margin should be included in the specified performance.

CALCULATION OF THE NETWORK ENABLED ISTAR PERFORMANCE ENVELOPE

To address some of the issues raised above, the UK has developed a database of IMINT and geospatial requirements that seeks to capture the needs for imagery in 2012. There are plans to extend this database to include other sources of intelligence, but useful analysis is already possible. Results so far indicate that, of the three critical parameters listed above, image quality is typically addressed most fully. Rather fewer of the specified temporal requirements can be met but it is the lack of adequate area coverage that prevents satisfaction of the 'largest number' requirements.

A more sophisticated analysis of the database would acknowledge that sensors might build up coverage over the desired region via a number of consecutive collection events, provided that the overall timeliness associated with the requirement is not exceeded. When the database is analysed in this fashion, the area and timeliness parameters can effectively be combined into a single metric: area coverage rate. The significance of this parameter is discussed in more detail below.

To be effective, an NEC must deliver information across all levels of command. (A system in which all the resources are allocated to the highest levels of command, for instance, would leave lower levels of command blind, and hence unable to perform their missions.) It is, nevertheless, the case that the concept of operations for a number of different ISTAR systems does make assumptions about the particular levels of command to which they may be subordinated. Bearing in mind the 'one-third, two thirds rule' (the military doctrine that each level of command should only expend one third of the time remaining before an operation before passing decisions to the next level down), it may at first seem incongruous that ISTAR assets could potentially be allocated to several different levels of command. This is because if a given ISTAR asset delivers appropriate data at an appropriate rate to one level of command, it might appear to be ill suited for other levels that would have different decision cycles. In practice, however, there are a number of factors that modify this initial conclusion. One is that the areas of intelligence interest will be different across the levels of command. Hence, a high-level commander with a large area of interest but a lower tempo of decision-making might actually demand data at a comparable area coverage rate to a lower-level commander with a smaller area of interest, who has much less time to make a decision.

Of course, other factors could modify this conclusion. One is that a high-level commander may be satisfied with the level of image quality that will identify large-scale force structures, whereas a low-level commander may require very detailed data for specific target confirmation. The relative priority of the different levels of command would have an influence on the proportions of the network-enabled resource allocated to different problems, as would the number of commanders demanding information at each given level. In addition, the rates at which data will be required will differ significantly between peace and war. All these issues can potentially be resolved via analysis of the requirements' database.

A more challenging problem arises when real-world constraints such as budget and detection probability are introduced. It is unlikely that the UK will be able to afford sufficient ISTAR to avoid having to set priorities. It is also unlikely that any realistic sensor would deliver perfect detection performance. In practice, therefore, the collection, coordination and information requirements management (CCIRM) system will still be needed. Although collocated, contemporaneous, comparable data are desirable as part of an NEC, an approach to resource allocation based solely on requirement priority could be very inefficient. This is because different sensors could well have different collection probabilities against a given target, with the result that, in an attempt to focus the network on the highest priority tasks, some sensors could spend significant periods deployed against targets they have little chance of detecting. Ultimately, the value of bringing a second collection system to bear on target A (to provide fusion data, say) must be weighed against the potential value of using that collection system against target B, which it might have a better chance of detecting, and so providing more information. It follows, therefore, that the efficacy of an NEC will depend critically on the accurate estimation and use of detection probabilities as part of a CCIRM algorithm.

EXISTING NETWORK ENABLED SENSOR SYSTEMS

There are many possible ways of defining what a network-enabled ISTAR capability should include. A potential short cut could be to find analogies in the natural world, where the biological sensing capability has been shaped by many thousands of years of evolutionary trial and error. Simply as an illustration, consider a human being as an analogue for a network enabled capability. A human's ISTAR system-of-systems comprises:

- **Hearing** – a medium and short-range semi-directional sensor, used for detection, direction cueing and some target recognition and identification.

- **Eyesight** – a short, medium and long-range, highly directional, stereoscopic sensor used primarily for target identification, recognition and technical analysis (though some moving target capability is provided towards the edge of the field of view). Much of the processing of such data is via change detection.

- **Smell** –primarily a medium to short-range sensor, used for target identification and analysis without much directional capability.

- **Touch** –a short-range sensor used for technical analysis and real-time target interactions.

- **Taste** –a short-range sensor used for the identification of specific, high significance, targets with which the human organism interacts most closely.

- **Thermal** – a short-range sensor capable of warning against the particular environmental threat of extreme heat.

It is interesting to note that there is a limit to the number of sensors with which evolution has equipped us, which suggests that the process has addressed the data-deluge problem. Most of our senses work at short ranges, where we can directly interact physically. This may be indicative of the need to bring three or more sensor systems to bear on the target acquisition element of ISTAR, over a performance envelope closely linked to the ranges of our weapon systems. Longer-range planning and target detection for humans depend primarily on two sensors, and again there may be a useful analogy here for military surveillance and reconnaissance functions.

Note also that the human senses listed above are underpinned to some extent by the proprioceptive sense, which is the human ability to determine one's current orientation/ position via sensors in the muscles. A military analogy for this sense of position would be an understanding of the disposition and state of readiness of one's own forces, which is similarly an underpinning requirement for the effective use of ISTAR assets.

CONCLUSIONS

Collocated, contemporaneous, comparable data are a central requirement for a network-enabled ISTAR system but this capability will not emerge without conscious and deliberate planning. To create an effective system-of-systems, it is essential to build collectors with intersecting performance envelopes in terms of range, timeliness and quality.

Different sensor systems will, inevitably, provide different capabilities. Analysis of the UK's requirements database will potentially allow an ISTAR system of systems to be devised that will deliver appropriate area coverage rates and data qualities for the different military levels of command. This system of systems will only be used effectively if detection probabilities are adequately taken into account in the CCIRM process.

G014, A2 Building, Dstl, Farnborough, Hants GU14 0LX
sjeves@dstl.gov.uk

Lessons for NEC from previous information systems initiatives

Jonathan Williams[1]
Information Management Dept, Dstl

Gerald Foley
KI Systems Division, QinetiQ

Abstract
Network Enabled Capability is the UK's initiative to enhance military capability through exploiting information better. NEC differs from other recent information systems (IS) initiatives in a number of respects, not least that it has support at the very highest levels in the Ministry of Defence. However, the challenges of delivering the UK's aspiration for NEC are considerable, and require coordinated action from a wide range of stakeholders and authorities. Gaining widespread support and sufficient management authority has proved elusive in the past, to the extent that many recent initiatives have failed to address the challenges fully and to deliver the benefits expected. This article seeks to identify both the problems and successes of recent initiatives so that lessons to be learnt can be successfully applied to NEC.

MILITARY CONTEXT

The military context against which the aspirations for NEC have emerged is described elsewhere in this journal [1]. In summary, the New Chapter of the Strategic Defence Review established an overarching priority to increase the emphasis on the integration of capabilities to facilitate the rapid and controlled delivery of precise military effect. The UK intends to achieve this by implementing NEC.

NEC brings together decision-makers, sensors and weapon systems, enabling them to pool their information by 'networking' to achieve an enhanced capability. It therefore encompasses the elements required to deliver controlled and precise military effect rapidly and reliably. At its core is a network to support the acquisition, fusing, exchange and exploitation of information. The NEC Conceptual Framework [2] sets out the background to NEC, characterizes it in greater detail, and charts the route towards its realization.

NEC is not the first major IS initiative: several over the last decade have each been heralded as offering unprecedented synergy, enabling truly 'joint' operation, or enabling our armed services to enter the digital decade. Each has received high-level support, a level of funding, and the enthusiastic commitment of military, scientific and acquisition staffs. Often, customer satisfaction has been lower than expectation. Why was this? Were aspirations simply too high in relation to technical feasibility or are there more fundamental reasons about how MoD seeks to deliver large-scale investments? We address these issues and try to draw some conclusions and recommendations for organizational structures, policies and programmes to ensure that NEC will deliver its intended advantages by exploiting information better.

METHOD

A workshop to address 'Lessons Learnt from Recent MoD Initiatives' was convened by the Command Control and Information Infrastructure System Concept Research project in January 2003. Its purpose was to inform those responsible for managing the delivery of NEC. Representatives from the MoD, Services and the research community who were involved in previous IS initiatives were amongst the attendees [3]. Amongst the programmes, projects and initiatives considered were:

- Defence Operational CIS Strategy (DOCISS)
- Command, Control and Intelligence Common Operating Environment (C2I COE)
- Joint Command System Initiative (JCSI)
- Digitization Stage 1 (DS1)
- BOWMAN and Digitization of the Battlespace, Land (DBL)
- Joint Battlespace Digitization (JBD).

A second workshop was held at Dstl Farnborough on 12 March. Although this was specifically to review the 'Bowman Within Digitization of the Battlespace Land (DBL)' report [4], it was also intended to inform discussions on NEC.

MoD's 'Customer 1' (the organization responsible for determining and managing future capability requirements) supported both workshops. The material presented and discussed has been analysed for common problems and successes [5]. Here, we present the key findings; it is hoped they will shape the will and resolve of MoD staffs to ensure the successful management and delivery of NEC capabilities.

KEY FINDINGS

A primary conclusion for successfully implementing NEC is the need for an effective management regime to communicate the benefits of NEC and to actively manage capability

[1] Jonathan Williams leads the NEC Delivery Team, a Core NEC project in the MoD's applied research programme, led by Dstl with support from QinetiQ and other industry.

integration activities. Other key conclusions are described below under six broad topic areas. However, it is acknowledged that NEC is neither a project nor a programme; it is to be implemented by the coherent acquisition of capability across many programmes. It is therefore essential that development is not restricted to equipment capability but that it also encompasses all the other 'Lines of Development' (LoDs)[2]. This suggests that the management challenges will be even greater than (or at best different from) previously. Hence, the policies, approaches and control mechanisms necessary may not be the same. Defence information systems have a history of initiatives that come and go, often one initiative evolving into another with a new 'brand'. This has resulted in a loss of impetus in addressing common and enduring features such as interoperability and integration, with many useful products and findings from these initiatives being lost. The NEC community should consider how best to retain momentum, and to maximize the long-term benefits of products, developed in the context of NEC, in a defence environment subject to inevitable changes of priority and direction.

System scoping and analysis

Many previous initiatives foundered during the system scoping phase where there was a tendency to focus on issues that proved to be unimportant. Too much effort was devoted to top-down, organizational analysis that was unlikely to be agreed or successful for capability programmes of large scale and agility. As responsibilities and programme needs change frequently, arguments on scope and definition contribute little to the overall business success. It is more important to understand the overall enterprise and the intended benefits any IS initiative is intended to deliver; thus the perceived benefits of NEC (even those that are inferred) need to be identified early and communicated to all stakeholders.

Key to delivering sustained improvement in military capability is the acceptance that NEC is a 'socio-technical' programme of capability enhancement where much of the benefit from information sharing will only be realized when methods of operation evolve in the hands of the user.

Financial planning

It has repeatedly been shown to be impossible to develop long-term financial plans for CIS projects. At present, financial and equipment approval mechanisms fail to take adequate account of the need to fund future system developments that are inevitable in the medium term, but cannot be well defined in the short term, when a decision is needed to commit funding to acquire an initial capability. It is evident that, if systems are to be developed incrementally, headroom for future development should be included in future capital and operating budgets from the outset.

Balance of investment decisions are also made more complex, and potentially invalid, by the distinction between 'systems' and 'infrastructure'. The equipment approvals process has to improve how it values the enhancements provided by infrastructure and enabling capabilities. The contribution that these make to overall military capability is often difficult to measure. Together with a better understanding of the whole-life cost profile for information systems, this would enable realistic funding profiles for these essential investments to be justified and approved. Integration is a through-life issue and a major component of through-life cost. The NEC core theme of inclusive flexible acquisition [2] will necessitate incremental capability development being far more responsive and iterative than in the past.

Delivering capability

There has been an understandable tendency to focus on equipment capability; delivery of NEC will require equal emphasis across all LoDs. NEC and the benefits claimed for it, perhaps even more so than in previous initiatives, need to be thoroughly understood by both Customer 1 and Customer 2 communities. (Customer 2 represents the needs of the end 'user' during the acquisition process.) This requires common intent to be developed between Customer 1, Customer 2, and also with the Defence Procurement Agency (DPA) and research communities. Experience from previous programmes suggests that unrealistic or unattainable levels of detail should not be sought too early –indeed, this can be an impediment to progress. Instead, the focus should be on managing cross boundary issues, and the mechanisms to develop, maintain and protect NEC 'System of System' Capability Requirements. Also critical is establishing a common high-level approach and overall plan for delivering NEC, matched by incisive and active management by both Customer 1 and Customer 2. A culture must be developed where we accept the need to 'plan for change' and where managerial structures are established to manage the frequent perturbations that will occur if we embrace the opportunities offered by information-age technologies.

Programme management

NEC, as for previous initiatives, may be considered as a system of systems, with a need for some degree of management at a programme (of projects) level. In the past, too much attention has been paid to describing methodology and project organization rather than making progress on those actions needed to offer explicit guidance to component projects. A Programme Management Office (PMO) or Programme Coordination Office (PCO) has sometimes been established. While any PMO (however effective) may be better than none, a PMO without appropriate authority is unlikely to be of any real value. Consideration should be given to establishing this function where, and only where, there is sufficient authority for effective action. Where adopting a PMO has been successful (for example, the DS1 and DS2 PMOs[3]), the scope of responsibility was well bounded and therefore the necessary authority established.

NEC will be a progressive, iterative and incremental acquisition that demands hands-on 'integration of capability'.

2 The Lines of Development are: Concepts and Doctrine, Equipment Capability, Structure and Processes, Personnel, Collective Training, and Sustainment.

3 Land Digitization Stage 1 (DS1) and Land Digitization Stage 2 (DS2)

As this will clearly be a key function requiring continuous, coordinated action, it is appropriate for Customer 1 to lead and for that function to be resourced with adequately skilled staff. MoD cannot contract-out the risks inherent in defence capability integration. Instead, it should take measures to manage those risks, perhaps with an industry partner, in particular to consider the risk trade-offs and palliatives across projects and programmes. Consideration should be given to establishing an 'integration architecture' role, something often lost in previous programme initiatives.

Acquisition (considered further in [6])

The 'Smart Acquisition' process requires the MoD, its agencies and services to work satisfactorily together. Using present mechanisms and structures, NEC cannot be delivered if responsibility for implementation is delegated to one part of MoD, whether Customer 1 or DPA. There is a need for continuous day-to-day management of the delivery of NEC to ensure that we do not over rely on committee structures for delivery. With emphasis being placed on experimentation, and incremental acquisition, greater flexibility is required in both capability management and acquisition. Without the single or lead-project level focus afforded by some previous initiatives, this will be particularly challenging to the implementation of NEC. Experimentation and flexible, responsive acquisition will be vital if the aims and objectives of NEC are to be achieved.

NEC, in common with previous initiatives, is based on a paradigm of infrastructure / application separation. While such an approach is in line with current trends in information systems, it has led to some difficulties in the integration of infrastructure and application components delivered by different projects. To avoid such difficulties, a stable specification of any target infrastructure is essential and it is recommended that early integration testing on target infrastructures, even during early development phases, is essential if these integration risks are to be properly mitigated.

Technical management

Integration and interoperability are intrusive activities that require continuous technical management. They inevitably constrain system designers. This may be offset by the use wherever possible of open, *de facto*, standards where these become the natural choice and are more readily accepted by such designers. In the past, MoD has found it impossible to mandate or enforce standards. Hence, a pragmatic approach to *de facto* commercial standards may be necessary, together with open, bespoke solutions to some of the military specific needs. In today's COTS-dominated environment, market watch is as important as technology watch.

Experience has shown that it is beneficial to concentrate early on the taxing problems, rather than to avoid the 'difficult' areas (for example, security or limited bandwidth) and that early selection of solutions or architecture may inhibit system growth. The early involvement of end users is often essential but their contribution may be ineffective unless they have the appropriate expertise and experience that can often only be found in operational units.

SUMMARY OF FINDINGS

Many of the above findings are 'managerial'. For those involved in previous IS programmes, this may not be news! However, one of the major differences between NEC and previous initiatives is that there will be no single or lead NEC programme, project or system. This places even greater emphasis on the need to manage and integrate capability successfully. As we have shown, many recommendations could be drawn from analysing lessons from the past. Hence this article focuses on the principal messages that require action from within MoD to take NEC from conceptual thinking to development action.

Maintaining momentum

Previously, many information systems initiatives have tended to lose impetus, and re-branding has not been uncommon. In particular, many useful products such as improved interoperability and integration have been lost. Experience has shown that momentum is lost when the taxing problems are not addressed in a timely manner. Those leaders responsible for NEC must ensure that structures are established to ensure that the initial successes over the past 12 months are maintained and that the organization can tackle the difficult technical, managerial and investment decisions that lie ahead. This should not be restricted to short-term fixes but must include the development of a long-term plan for exploiting the opportunities offered by information-age technologies and more beneficial tactics, techniques and procedures.

Communicating NEC

The intended benefits of NEC should be clearly developed and articulated such that NEC is made understandable to all defence stakeholders (including industry). A commonly agreed high-level approach and overall plan for delivering NEC should be established. These steps will help to allay some of the concerns expressed about the lack of a central focus, will avoid the likelihood of 'NEC fatigue', and will enable all stakeholders contributing to NEC to understand how best they can contribute to its successful delivery.

To complement this high-level plan, NEC will benefit from definition of a suitable architectural framework that helps to guide the implementation of planned and future capability. This framework should provide readily accessible views (or multiple views) of the future equipment capability, and its corresponding connectivity, integration and interoperability needs, that can be contributed to and shared by all NEC stakeholders.

Capability integration

There is a need for effective 'capability integration' led by Customer 1. This demands rigorous, expert, examination of capability, spanning traditional system and organizational boundaries, and will require a Customer 1 having a competent understanding of the equipment programme and its inter-relationships with other capabilities. MoD should invest in developing a system architect role within the equipment capability customer organization with the responsibility and authority to develop and maintain coherence of programmed investments in NEC.

Fundamental to delivering sustained improvements in military capability is the acceptance that NEC is a 'socio-technical' programme of capability enhancement. Thus it is imperative that capability and equipment solutions are co-evolved in concert with the operational staffs responsible for implementing the new equipment into service and evolving its ways of operation.

Maintaining the technical vision

The NEC 'core themes' re-enforce the acknowledged challenges of capability and system integration, interoperability and process development. Continuous technical support will be needed to ensure that the NEC vision is maintained and developed to support the delivery of NEC capability. This requires MoD to harness extant research, experimental and study capabilities, and teams from across the defence community to develop and maintain system of systems capabilities that will lead to continual enhancement of military capability by the better exploitation of information.

Programme management

MoD cannot contract-out the risks inherent in defence capability integration. Hence, it should take measures to manage those risks. Capability stovepipes are primarily the result of the requirement to exchange information and services being excluded from the system requirements, or being traded out by investment decision-makers to achieve savings. Successful delivery of NEC will require that 'platform centric' attributes do not gain pre-eminence over 'network enabling capabilities'. For that reason, a key role of Customer 1 must be to ensure that enterprise-level capabilities are not compromised during the acquisition process and continually to look across the boundaries inherent in the capability management organization, orchestrating trade-offs to improve overall military capability.

Accordingly, it is clear that an effective NEC programme management regime should be established. Wherever this responsibility rests, it will be apparent that the nominee must have appropriate authority and also be properly resourced to manage the delivery of NEC satisfactorily. This function should be established where, and only where, adequate authority can be established.

Balance of investment

The equipment approvals process should be further developed so that enhancements provided by infrastructure, and enabling or synergistic capabilities, may be properly valued. This will require the process for analysing investments in capability (particularly equipment) to be re-examined. As we increasingly move into an era of effects-based operations, the suitability of current sets of pre-contextualized and attrition-based scenarios forming the basis of investment planning must be carefully considered.

Experience has also shown that it is virtually impossible for approval mechanisms to enable provision to be made for future system developments that cannot be adequately defined in the short term. The equipment approvals process should be re-examined since many of the capability advantages offered by NEC will demand the rapid insertion of new technologies that cannot be articulated some time ahead.

Integration and interoperability

Integration and interoperability are intrusive activities that inevitably constrain the solution space open to system designers. MoD should adopt a pragmatic approach using and accepting *de facto* commercial standards wherever appropriate.

Early integration testing should also be planned so that separately developed applications can be adequately tested on representative target infrastructures. This will help MoD to characterize the value and benefits of the underpinning infrastructure and services, and to prove the deployability and utility of the candidate applications.

References

1 Ferbrache D. *Network Enabled Capability – concepts and delivery*. J Defence Science **8** 104 (2003).

2 Alston A. *Network Enabled Capability – the concept*. J Defence Science **8** 108 (2003).

3 The proceedings of the workshop are contained in Dstl/IMD/SOS/500, Lessons Learned Proceedings (25 Jan 2003).

4 D/DDOR(Pol & SP) 111/1 (17 September 1999).

5 Dstl/IMD/SOS/500/2, NEC Outline Concept, Issue 2.0 2: Part 8 - Managing the Successful Delivery of NEC (May 2003).

6 Ellis R. *Can Network Enabled Capability be delivered?* J Defence Science **8** 160 (2003).

Information Management Department, Dstl Portsdown West, Portsdown Hill Road, Fareham, Hants PO17 6AD
JPWILLIAMS@mail.dstl.gov.uk

NEC –the implications for acquisition

Peter Brook and Rob Stevens
Integration Authority, Defence Procurement Agency

Abstract
The key to achieving NEC is change, to acquisition no less than to communications, weapon systems and command. Moreover, acquisition is the visible face to the world where shortcomings accumulated en route conspicuously affect perceptions of the success of the enterprise. In describing in broad terms the background to procurement implementation philosophy and plans, the paper identifies familiar challenges in achieving integration and outlines approaches to their containment, some of which are already in hand. Necessarily, because the paper looks ahead against a background that is not entirely defined, the only certainty will be the need to work to an overall synchronized plan, while maintaining flexibility and the ability to make adjustments. The key to success will be wide acceptance of the NEC culture and the will to make it work.

INTRODUCTION

The advent of NEC as the aspirational goal of MoD is a direct result of developments in communications, computing and sensing that have opened up unprecedented opportunities for more complex 'meta systems', which may work together to provide greater tempo and agility to the operational commander. These are amply described by others in this journal. However, the connectedness of the systems themselves places huge demands on the whole acquisition community, which has been brought up to treat systems - and the projects that bring them into being –as largely separate entities. The Smart Acquisition reforms of recent years, while bringing wholly beneficial clarity to roles and responsibilities, and a better corporate approach to risk management and accountability at the individual project level –have done little to tackle the issue of connectedness, and in some ways might even have made it more difficult.

Responding to these challenges, and taking the opportunities NEC offers, will require a far greater cohesion across the Enterprise of defence. It will no longer be possible to treat integration as an add-on or optional feature, and the impact is likely to be felt in a range of novel organizational responses. This paper, echoing the thoughts of the other authors, will present an acquisition-wide perspective of the scale of the challenges, expressed initially in conceptual terms, discuss what might be required as a medium-term response, and describe some of the first steps that are being taken in the required direction.

NEC INTEGRATION FROM AN ENTERPRISE PERSPECTIVE

Integration may be defined as '*The act of combining or adding parts to make a unified whole*'. This definition implies that integration needs must be expressed with respect to a unified whole and that understanding its scope is critical to success. The concept of adding parts implies the presence of an existing part, or legacy, to which others have to be added in a coherent and coordinated way and, by implication, the adding of a number of parts simultaneously. These issues – scope, legacy and simultaneous change –are the recurring themes of this paper.

Defining the Enterprise of Defence –which is the context for NEC, and the business it aims to transform –is difficult to do in precise terms, given the scale and complexity of the organization. A recent workshop suggested the following:

> *'The Enterprise is what Defence does in its widest context: the core of MoD and Armed Forces involving OGDs*[1]*, industry, allies and others in executing the processes and activities necessary to deliver the Defence (and NEC) Mission.'*

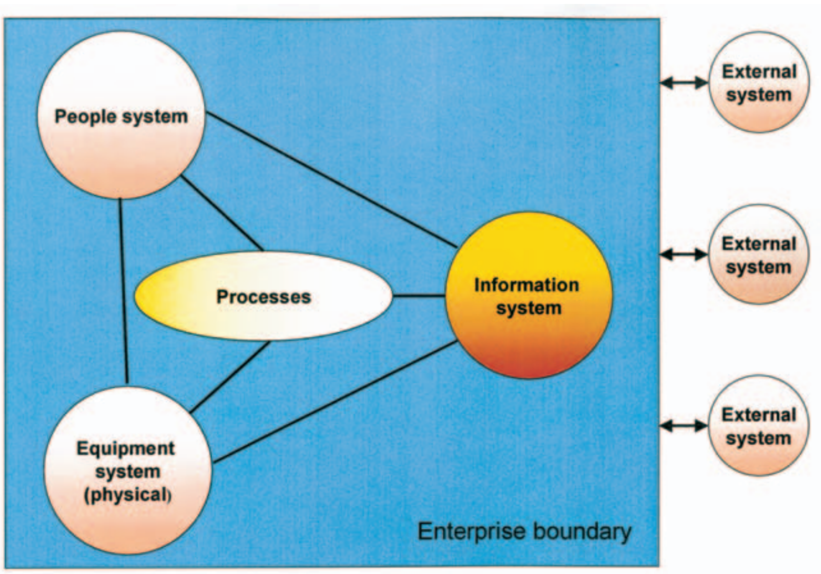


Fig 1. A generic model for the Enterprise of Defence

[1] Abbreviations that might be unfamiliar to some readers are expanded on page 178

It therefore comprises its people –including armed forces, civil servants and embedded contractors – working with equipment and information systems. Externally, it works with OGDs, NGOs, industry, the public, allies (individually and collectively) and the political systems. (Figure 1.)

Interestingly, and significantly, the same figure can be used to depict the (embedded) Acquisition System, which in its broadest sense is the business responsible for bringing about the changes that transform the Enterprise. It too comprises its people (the Acquisition Stream as a whole), processes (the Acquisition Management System), information systems (about projects and systems, as they are developed and used) and equipment systems (which assist with building and testing the equipment and information systems). It is evident to many in the community that we shall require simultaneous transformation of the acquisition community to effect the NEC vision. And, just as the systems we build will have to be integrated with those of our significant allies in the operational domain, so our acquisition activities will have to be harmonized along the same lines if this is to be achieved.

Two factors are important in achieving and maintaining integration at the Enterprise level: the level of intricacy of the Enterprise (driven by the scale and complexity of the systems) and the rate of change needed to respond to changes in mission and technology (ie, requirements and opportunities) which in turn is driven by greater uncertainty in mission and available options. The relationship between them is shown in figure 2.

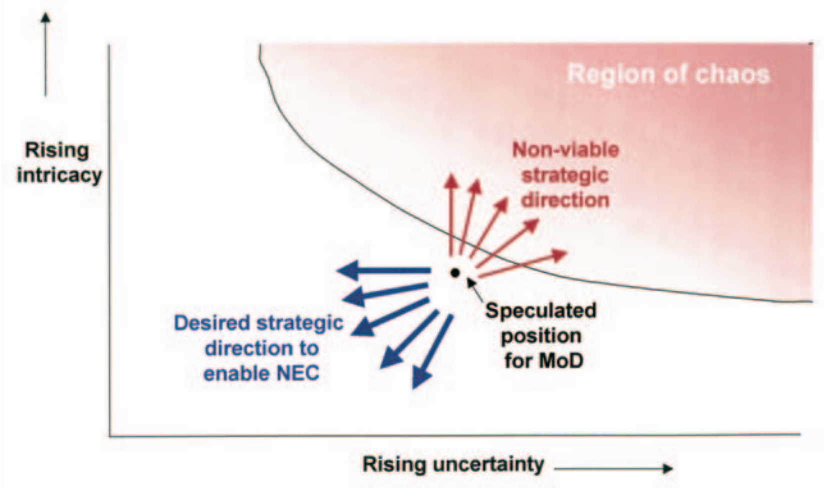


Fig 2. Intricacy, uncertainty and the avoidance of chaos

Where intricacy and uncertainty are both high, the rate of change required by the acquisition system can be faster than the rate at which stable change can be delivered. As a result, the Enterprise may be unstable when further change is applied, requiring further resources to maintain integration to support on-going business continuity needs. In the worst case, a point is reached where the organization does not have the resources to maintain either. Although there is no firm evidence that MoD has reached this point, lessons learnt from current operations suggest that this danger is real. A more structured and coherent approach in the application of further changes will, in the opinion of these authors, be essential to the achievement of NEC.

In the area of intricacy, the MoD Enterprise contains many systems, usually stove-piped and few, if any, well characterized. End-to-end services are provided by pragmatic means, often in the operational domain, by patches and work-arounds. We therefore have in existence a complex web of connectivity, dependencies and responsibilities. This will have to be stabilized by the introduction and adoption of a number of Enterprise Architectural rules that can reduce component coupling and stem the unchecked build-up of intricacy. Experience in the design of large-scale information systems has shown this to be the only feasible approach.

Uncertainty is inherent and has to be coped with. Few could have predicted three years ago further Afghan and Second Gulf expeditionary wars, and yet many of the systems used were designed against Cold War scenarios. The timescale of response required has been well inside the decision loop of our acquisition change activity, leading to a plethora of Urgent Operational Requirements (UORs), which themselves have further added to the complexity of the deployed systems by not being harmonized with the design of those in the acquisition pipeline. Further rework at the integration point is almost inevitable. A broader coping strategy would have to include handling of expected change in a more evolutionary manner and designing for unexpected change by adopting agreed open systems architectural approaches. To make this feasible, the organization will require an Enterprise Evolution Plan (EEP), working with the Enterprise Architecture as a key enabler, for managing and coordinating short-term responsive changes in a coordinated manner.

CURRENT STATE OF ENTERPRISE INTEGRATION

It is salutary to compare MoD's current position in more detail against the generic model just described. Experience to date suggests the following difficulties in our present approach, in no particular order, that will have to be overcome.

- ***Activities of individual IPTs not harmonized***.

In general, IPTs handle their integration activities well, especially when they are scoped within an individual portfolio, but less so than the information chains they support span IPT boundaries. Here, smart acquisition processes have had little to offer to date on the subject. Clear progress has been achieved with the emergence of through-life IPTs (covering an area of capability from initial acquisition to operations and able to handle continuous up-grade in a more coherent manner), service delivery IPTs (for large infrastructure programmes, especially in the strategic and fixed domains) and Integrating IPTs (for example, bringing together applications, infrastructure and communications from a number of teams and managing them as a whole). However, residual uncertainty in their integration boundaries persists, and could grow unless checked.

- ***Integration of programme products into the MoD Enterprise***.
  The establishment of Programme Management processes, pioneered by the IA and BLD IPT for the delivery of Command & Battlespace Management (CBM) Land, have provided a new model for how a group of projects can be organized architecturally by epoch and managed as a whole. Much practical experience has already been gained in the more novel operation of across-IPT and across-contractor working that can be extrapolated into other groupings, such as those that will comprise NEC. However, there is currently no mechanism to integrate a number for these epochs into the Enterprise, or to ensure that their cumulative impact on the operational domain on Transfer to Operations (TTO) does not lead to loss of capability, albeit temporary.

- ***Synchronization of enterprise change mechanisms.***
  A number of change mechanisms affect the MoD Enterprise. These include: major acquisition, upgrade, maintenance, reconfiguration, redeployment, failure, operational damage, UORs and disposal. The coordination of these into a platform is complex but the issues are generally under control. The picture is not so positive for MoD-wide information systems, where end-to-end value chains are fragile and can be damaged by uncoordinated changes in single parts. The solution will have to be sought in the area of better diagnostic and rectification mechanisms at the pan-system level.

- ***Coordinating activities with different response times***.
  Major platforms and equipments may take many years to bring to fruition. Parallel changes to the Enterprise may invalidate the assumptions on which their requirements were initially based. In consequence, the Enterprise may look quite different at the point at which it is ready for operations, with consequent difficulties in achieving integration. Currently, there is no effective mechanism to constrain short-term initiatives to ensure integration with the longer-term programmes, or to evolve major acquisitions to hit the moving target of the Enterprise at the point where TTO is envisaged.

- ***Coherence of requirements.***
  Because of the sheer size of MoD, many requirements documents (URDs and SRDs) are current at the same time. The aim of a URD is to ask for a change to the Enterprise at the time the desired capability is introduced into service, and so requires a view of how it will look at that point to ensure compatibility. Faced with this problem, many URD writers fall back on a spurious sense of certainty, which the organization often calls for in order to give approval and to monitor progress, or to ignore such factors altogether. Integration issues could be assisted if the exact scope (relative to the Enterprise) could be expressed up front, along with constraints and external dependencies, and such assumptions held in the URD.

- ***Trade-off mechanisms***.
  Trade-off is neither well understood nor coherently conducted at the Enterprise level. Individual IPTs and DECs understandably use the opportunity to conduct further trade-off at the project level, in the absence of knowledge of the wider impact.

- ***The coupling of physical and information systems within acquisition***.
  Platform-centric acquisition often results in the platform's information systems being tightly coupled to the platform acquisition. The reasons are entirely clear and understandable: to overcome the high-profile failures of information-rich platforms of the past, the MoD has sought to place whole system responsibility with the platform contractor. As the complexity (and relative cost) of the embedded information system grows, along with its connectedness to the wider information system, this coupling becomes problematic.

- ***Business continuity impact caused by transition to operations***.
  The Enterprise is an evolving entity. It is continuously in service in some form or other, and demands business continuity. Integrating new capability can be disruptive, especially if the intricacy is high. It should be possible to trade off the benefits to be gained by introducing new capability with the risk of potential disruption, though this is rarely done.

- ***Management of reconfigurations of the delivered system***.
  The current intricacy of the MoD information creates value chains that otherwise might be independent. A request for a change to one –for example an increase in bandwidth, or provision of a resilient route –may have an adverse effect on another. Unless managed, the result can be low-level churn. Integration at the point of TTO does not prevent later churn as reconfigurations and redeployments take place. One of the many mechanisms required to achieve stability is a coordinated system management function. But this can only succeed if adequate initial Enterprise design has taken place.

- ***Synchronization of the Lines of Development***.
  To meet the Enterprise vision, it is necessary to consider how benefits might best be achieved by exercising all the degrees of freedom at the Enterprise level. In particular, it is necessary to understand how changes to people, equipment, information and operational processes may maximize benefit using the lines of development as a check to see they are all covered and synchronized. The current separation of these mechanisms is a considerable source of risk.

TOWARDS A MODEL FOR ENTERPRISE INTEGRATION

Rectification of the above problems requires the establishment of a number of new processes, many of which already exist in partial or embryonic form, and their coherent introduction at the Enterprise level. The concepts of an Enterprise Architecture and an Enterprise Evolution Plan (EPP) have already been referred to. The key processes that would surround their application are illustrated in figure 3, and comprise:

- ***Enterprise needs process,*** which identifies enduring needs and drivers, including the need for change and stable assumptions that can be used for architectural development
- ***Enterprise architecture process,*** which formulates and maintains a coherent architecture across all lines of development, to support an Enterprise Evolution Plan, and the formulation and maintenance of the EPP itself, containing sufficient granularity to control Enterprise Integration
- ***Enterprise design process,*** which formulates new design solutions within the constraints of the existing EPP, conducts trade-offs to generate options for change to provide requirements for action by the realization process; these will form the high-level requirements for major acquisitions
- ***Enterprise control process,*** which sets overall direction and promotes change, and is ultimately accountable for the effectiveness of the Enterprise
- ***Enterprise realization process,*** in which changes are brought about to individual programmes and systems, and new ones created
- ***Enterprise governance process,*** which assures that risks are understood and managed, that projects maintain conformance with the architecture and the plan, and unplanned events are catered for
- ***Release management process,*** which coordinates the introduction of new products, service and capability such that benefits are realized and ensures that Transfer to Operations takes place in line with the EEP
- ***Utilization process,*** in which systems and services are used, performance assessed and requirements for future Enterprise change fed back to the Enterprise needs process.

The change cycle is shown in figure 3 as a continuous loop in line with overall Enterprise evolution. Two underlying dynamic behaviours are present: the overall ***Delivery Cycle,*** which passes change requirements from utilization and control, through needs, design realization and back to utilization; and an ***Integration Realignment Cycle,*** which is enabled by the governance process identifying integration misalignments, and passes these through management, needs and design back to realization, where realignment can be actioned. The operation of these two cycles should result in a proportion of changes leaving the realization process in a form that will ultimately lead to integration success –a truly virtuous circle, which is shown in figure 4.

PRACTICAL FIRST STEPS

The model presented may appear abstract and beg the question 'where to start?' The authors' current organization, the Integration Authority (IA), was brought into being to address the integration agenda in early 2000, and has been making significant inroads into the problem. The work has entailed

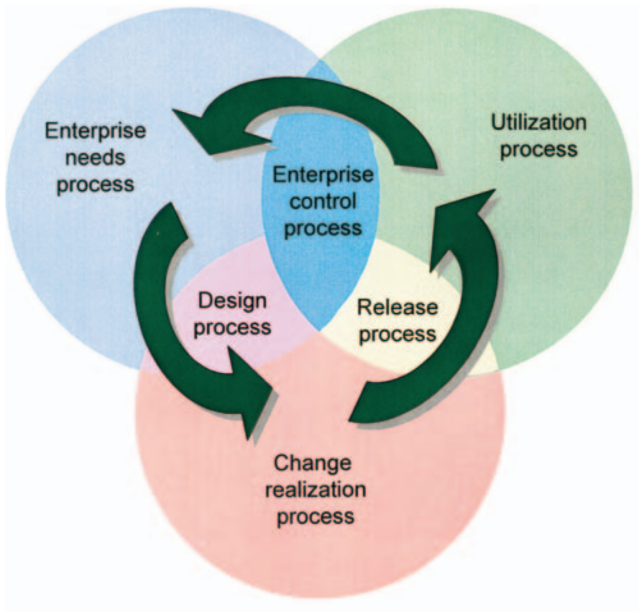


Fig 3. The Enterprise Change Process

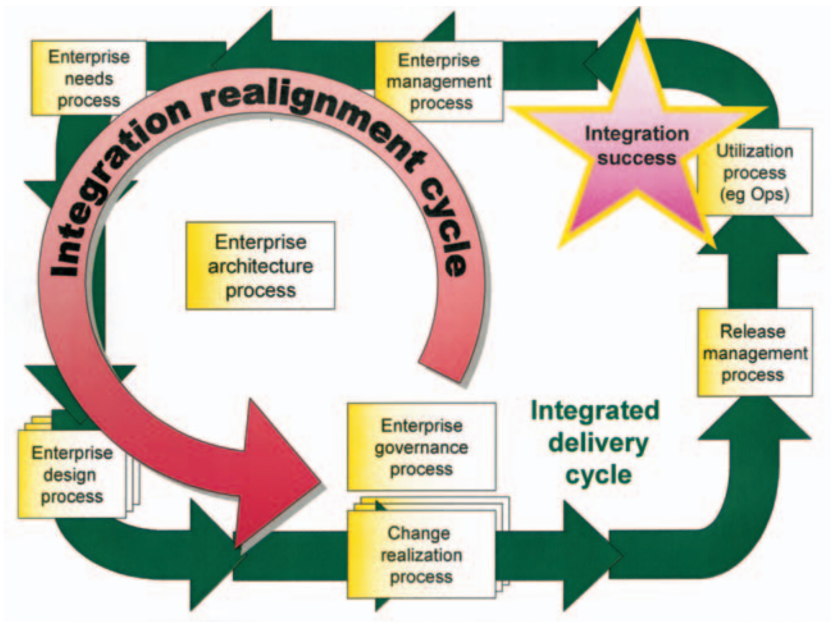


Fig 4. Feedback and realignment in the enterprise processes

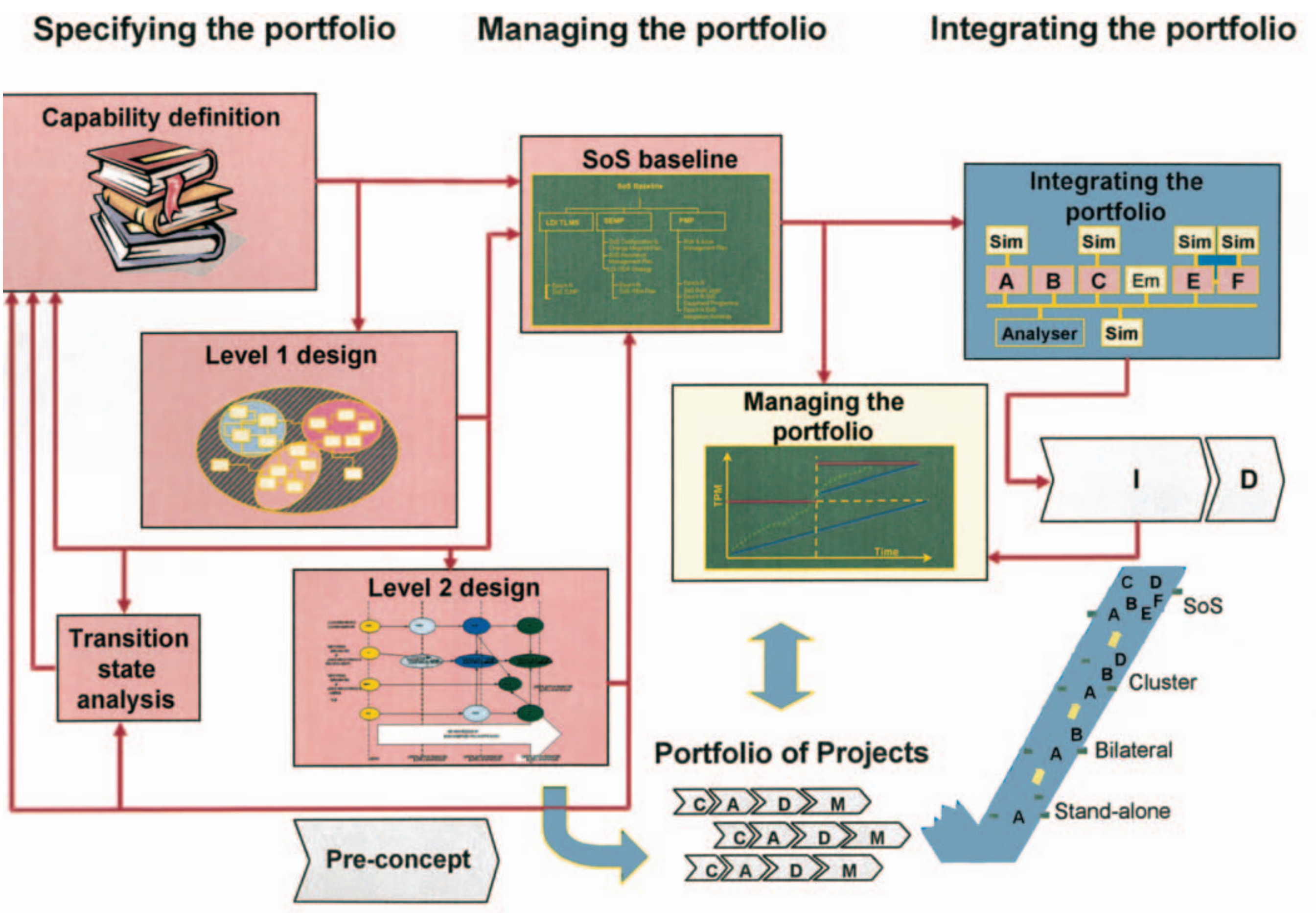


Fig 5. Systems of systems engineering processes

the simultaneous creation of new processes and models, while ensuring early delivery of some of the benefits of integration. The IA's programme has been undergoing major review in the MoD, based on a three-year forward programme comprising the following three strands:

Architecture: The IA has been designated as the 'Chief Technical Architect' in support of the Joint Capabilities Board (JCB), as an integral part of the move towards NEC. Current activities are focused on the generation and agreement of ***Enterprise Architectural Principles***, with suitable owners across defence and the IA being responsible for their coherence. New architectural processes, piloted and beginning to operate in the CBM Land programme, are now being published, which will allow future concepts and requirements to be fed into more coherently-aligned project groupings in the early stages. It is expected that NEC change programmes will increasingly conform to this model. Underpinning both will be the adoption of DoDAF[2] as the common architectural language, in which projects will be expected to express their requirements and associated views. (DoDAF allows projects and programmes –and their interactions –to be self-consistently depicted and modelled in a series of Capability, Operational, Systems and Technical views.) NATO-wide adoption is also expected.

[2] DoD Architectural Framework. Version 1.0, January 2003.

Governance: Still in incipient form, the IA is now operating a set of assurance processes to ensure that new projects and programmes reflect the architecture, and that knowledge of their key characteristics is fed into the corporate knowledge base. The guiding principle is that IPTs and others retain responsibility for delivery but will be required to seek assurance from the IA that their projects are aligned –at the early stages, at key review points and in the event of significant change. Risk management within the assigned integration boundary remains the IPT's central task.

Coherent interventions: Gaps in the portfolio of projects will inevitably arise from a number of sources: unforeseen requirements, or gaps arising from operations or the assurance processes themselves. The role of the IA will be to ensure that these are filled in a coherent manner, again working as far as possible within the Enterprise architecture to ensure downstream business continuity.

To enable this programme to take place, a number of supporting workstreams are also under way:

Process development: Reference has already been made to the need for parallel process change, and the IA is teaming with DG Smart Acquisition to enable this to happen. In simple terms, the IA continues to lead on technical process development and DGSA on behavioural change and rollout. Current discussion centres on short-term improvements in assisting customers and IPTs to express coherent requirements (URDs and SRDs) aligned to the DoDAF model; roll-out across the community represents a significant change management programme, and will have to be planned and supported as such. More advanced work will involve more general application of 'systems of systems' processes at the multi-project level, creating a more formal model for the Integrating IPT. Figure 5 shows the sort of multilevel design processes, currently being developed for us, by which groups of projects comprising a portfolio are progressively designed and managed as a whole.

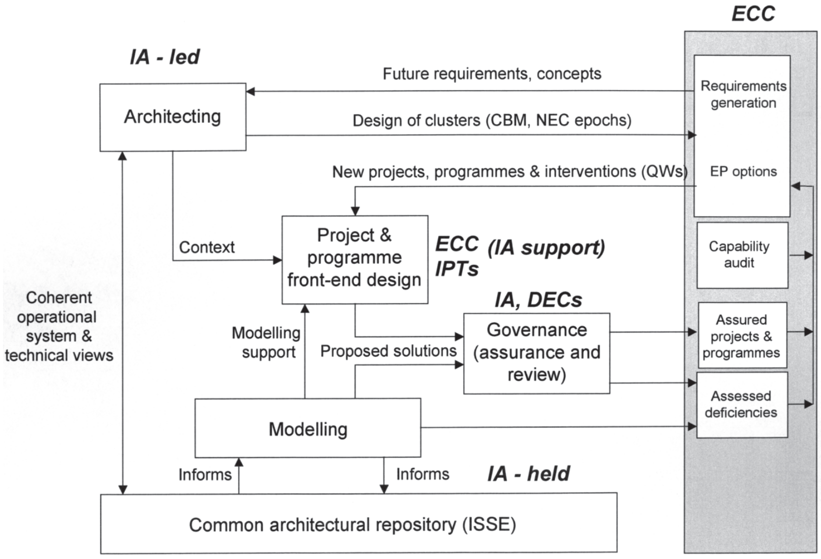


Fig 6. A new front-end architectural process

Information management: Many of the current problems in handling integration across MoD stem from the lack of historical attention to managing project and systems information. The net result is that we are now launching new systems to integrate with largely uncharacterized legacy, 'within acquisition' systems and those at the concept stages. The IA has been making a major investment in a new information repository – ISSE (Integration Services Support Environment), which holds technical and programmatic information on key projects. A large data-gathering exercise was launched last year, with the result that we now have for the first time an emerging Enterprise view of our programmes and their relationships. Technical development continues to allow ISSE to depict DoDAF views and to enforce a unified reference model. Future plans include teaming with DCSA (Defence Communications Services Agency) with a view to their managing compatible views of current operational systems, which can be exchanged with the IA. ISSE is already being made available to IPTs and their contractors, and its use is confidently expected to grow across the acquisition community, with consequential improvements in organizational clarity – itself an uncertainty-reduction measure – not to mention savings in the time and costs of multi-project data gathering.

Modelling: As the Enterprise infrastructure grows, and greater demands are made on its capacity, especially by the more time-sensitive elements of NEC, it will be necessary for the organization to model the major systems' interactions and communications' loadings at key stages, in particular at initial design and before major deployment, and when major configuration changes may take place. The IA is teaming with DAES and industry to create more unified modelling and experimentation environments, and to integrate them more fully into the acquisition process.

Integrated Test and Evaluation: Often the poor relation, the Test and Evaluation world will become increasingly important to Release Management, and will itself need to become further integrated if it is to be able to test the more complex meta-systems that NEC requires. At present, the IA is working on a plan for the better coordination of Test and Reference centres devoted to the acceptance of Command and Information Systems. In time, the concept will need to be extended to include those facilities and ranges that are responsible for the weapon and platform programmes that find themselves in-the-loop for NEC.

How some of this might come together in the near future is shown in figure 6, as new front-end design processes are established to harmonize new projects or project groups at the early design stages, with feedback into the processes governing the oversight of the Equipment Programme (EP) in the Equipment Capability Customer (ECC) area.

Putting these pieces together, we envisage the NEC transformation world to comprise larger NEC programmes

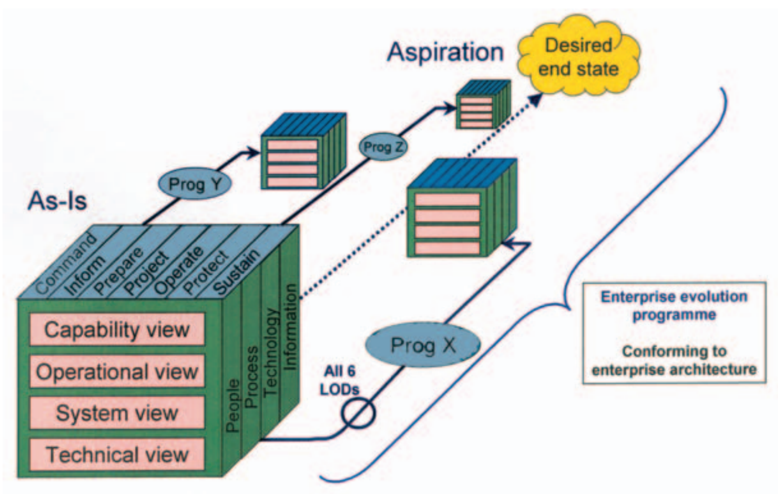


Fig 7. Simultaneous NEC programmes

being coordinated into manageable groupings, each comprising multiple lines of development, modelled in a consistent manner at the initial stages and managed under the overarching control of an Enterprise Plan and conforming to an Enterprise Architecture. Figure 7 shows our current thinking about how this might look. NEC programmes might, for example, comprise major infrastructure insertions, whole systems upgrades (for example, introduction of a common Internet layer across the battlespace down to the platform level to enforce information exploitation) or specific NEC thrusts, such as kill chains.

There are a number of major features missing, which will have to be attended to. These include formal release management mechanisms to assure system upgrades, and technology to facilitate better dynamic reconfiguration on deployed systems into multiple operations. Perhaps most pressing is the need to further understand, characterize and where necessary rationalize the existing infrastructure to reduce the complexity of the future integration challenge. The Defence Information Infrastructure (DII) programme is a major step in this direction. The result may well be further rationalization of project and programme boundaries, against a more logical model.

Last but not least are the people and skills issues involved in providing an acquisition workforce, in all areas of the MoD and the wider Enterprise of Defence, capable of managing the complexities involved.

CONCLUSIONS

This paper has painted a broad picture of necessary changes to acquisition that will be essential to the achievement of NEC, along with some of the initial investments in the novel underlying concepts. To bring these about will require many of the same features – for example synchronized decision-making, shared information and agility – to be applied in parallel to the acquisition systems. It is difficult to be sure how this will look in just a few years time. Some of this vision was foreseen in a previous paper[3]. Then, as now, it was not difficult to discern the direction of travel; it is much more difficult to predict how far and how fast MoD will travel, which depend on a combination of will, effort and investment, cohesively applied. And because the implementation issues are complex, especially at the Enterprise level, and therefore inherently unpredictable, we shall have to approach this in sensible-sized steps. The destination is bound to look different when we are further down the road.

Glossary

AMS	Acquisition Management System
BLD	Battlespace and Land Digitization (IPT)
CBM	Command and Battlespace Management
DAES	Director of Analysis, Experimentation and Simulation
DCSA	Defence Communications Services Agency
DGSA	Director General Smart Acquisition
DEC	Director of Equipment Capability
DoDAF	(US) Department of Defense Architectural Framework
EA	Enterprise Architecture
ECC	Equipment Capability Customer
EEP	Enterprise Evolution Plan
EP	Equipment Plan
IA	Integration Authority
IPT	Integrated Project Team
ISSE	Integration Services Support Environment
JCB	Joint Capabilities Board
NGO	Non Governmental Organization
OGD	Other (non-MoD) Government Department
SRD	System Requirements Document
TTO	Transfer to Operations
UOR	Urgent Operational Requirement
URD	User Requirements Document

3 Brook, P 'Systems Engineering for the Next Millennium', J Defence Science, Volume 5, Number 1, January 2000

Integration Authority, Defence Procurement Agency, Abbey Wood, Bristol
IA-GL@dpa.mod.uk

The UK approach to future Command and Inform (C4ISR)

Paul Robinson and Lt Col Iain Pickard
Joint Doctrine and Concepts Centre

'The command system.will remain a key force multiplier and advantage..opponents will seek to contest this through electronic warfare, computer network attack and asymmetric techniques' [1]

Abstract
Recent work at the UK Joint Doctrine and Concepts Centre has concentrated on developing a future High-Level Operational Concept for UK Armed Forces to articulate how the components of the Defence Capability Framework[2] *(Command, Inform, Operate, Prepare, Project, Protect and Sustain) will be realized and harmonized out to 2020. We first examined the strategic environment and the nature of future operations. We then looked in detail at the nature of future Command and Inform (C&I) to give a framework for the other components and, more particularly, to give a conceptual basis for the significant investment now being made in Network Enabled Capability.*

FUTURE ENVIRONMENT

Although the risks of armed conflict on a Cold War scale may be lower, there is increasing turbulence world-wide, with persistent mid to low-intensity threats, a trend that is likely to continue. Threats will increasingly include terrorists, rogue states and other non-state actors who may not be easy to identify or locate. None of these is likely to observe international law and moral conventions. We can expect asymmetric attacks on our strategic and operational centres of gravity but across a much wider battlespace[3]. At the same time, globalization, the interconnection of world-wide resources, economics and information, will create conditions where intentional effects can lead very rapidly to unintended consequences. Potential adversaries will rapidly adapt to this complex environment, where cause and effect will be hard to predict. We shall face adversaries whose structures lack traditional nodes and whose centres of gravity will be hard to define and attack[4]. They may choose to operate where our strengths are weakened and theirs are maximized, such as the complex terrain of urban areas. It is judged that there will increasingly be a move away from a geometric, Jominian[5], model of the battlespace toward a model that is non-linear and non-contiguous in both space and time.

Arguably, the structure, processes and equipment of the UK Armed Forces remain best suited to operations against symmetric adversaries in a geometric, industrial-age, battlespace. There is, therefore, a compelling need to adapt to the new environment and move away from forces that are physically and conceptually heavy, relatively inflexible and strategically immobile, toward lighter, more agile and mobile forces. Although UK Armed Forces should remain optimized for warfighting, trends derived from recent operational experience indicate that we shall still need to undertake a wide range of other operations, from peacekeeping and counter-terrorism, to power projection and deliberate intervention. The full range of operations may take place simultaneously in the same battlespace, the so-called 'Three Block War'[6]. With 24-hour international media increasingly acting as a shaper of public opinion, we are likely to be called upon for rapid intervention to avert crises and to respond to humanitarian disasters.

> Our compelling need is to adapt to the new strategic environment

Operations in 2020 are as likely to be in *ad hoc* coalitions of the willing as they are to be with established allies. The technological capabilities of potential coalition partners will range from those who stay abreast of US transformation, to those who retain some form of interoperability, to those who do not. It is also likely that many non-military organizations with whom we need to operate in the battlespace will lack compatible C&I capabilities. Therefore, whilst technological interoperability is a major issue, culture, organizational structure, procedures and training will significantly influence the effectiveness of all organizations involved in joint or combined operations[7].

It is likely that tolerance in our society to friendly, adversary and civilian casualties, collateral damage and damage to the environment will diminish, whilst legal imperatives will increasingly constrain our freedom to operate and train. For sound legal and operational reasons in our pluralistic society, we shall require an audit trail of operational decisions and consequences. Adversaries, on the other hand, will rarely operate under such constraints, giving them an asymmetric advantage.

Against this background, emergent nanotechnology, information technology (communications, data processing and fusion, information collection, distribution and dissemination), power sources, satellites and advanced sensors, offer the potential to revolutionize our ability to command and inform. There is a growing realization, however, that although technology is rapidly delivering more information, the processes needed to manage this information have not kept pace:

> *'The Information Management challenge is about to overwhelm us"*[8].

If we are to maximize the leverage offered by technology, it will be necessary to prevent commanders and their staffs from being swamped by information; thus more efficient Knowledge and Information Management (KIM) techniques are required, which must encompass technology, procedures, training and structures. Current major science and technology thrusts in these areas are reviewed at Annexe A.

Network Enabled Capability

UK Armed Forces intend to exploit emerging technology through the adoption of a Network Enabled Capability (NEC)[9]. It allows us to exploit the potential of 'network' technologies and enables integration with emerging US concepts. NEC promises to deliver Shared Situational Awareness (SSA)[10], a condition where force elements achieve a common or, at least, consistent understanding of both the strategic and operational level contexts and the prevailing tactical situation. Despite advances in technology, however, information will never be complete. The electro-magnetic spectrum (EMS) will continue to be constrained by power, propagation, bandwidth and enemy action, and it is highly unlikely, therefore, that we could ever realize a complete picture of our own forces' dispositions and intentions, let alone those of an adversary. Military operations will continue to be characterized by a degree of uncertainty; the so-called 'fog of war'. This uncertainty will be exacerbated by the political imperative for speedy decisions. These two factors together mean that, as today, many critical decisions will continue to be made on the basis of incomplete information. Furthermore, although blue forces will gain advantage by degrading an adversary's C&I capability, reliance on advanced C&I capabilities represents an increasing vulnerability. This vulnerability can be considered in three specific areas: systems attack (to which COTS technology is likely to be particularly vulnerable); intrusion and misinformation (whose effect will be magnified by networks); and the danger that the uninformed may have unrealistic expectations of a 'high tech' military's ability to achieve success at minimal or no cost.

FUTURE OPERATIONS

UK Joint Vision seeks to realize the full potential of the manoeuvrist approach[11] and articulates Effects Based Operations (EBO) as the best way to achieve this. EBO are focused on actions and their influence on behaviour, rather than simply on targets and attrition. The concept is not new; good commanders have in the past intuitively understood and applied a wide range of effects, but it is intended to develop a system that will deliver the right effect more consistently. It is envisaged that a lexicon of effects will give specifics, such as reassure, persuade, deter, coerce or destroy. The overriding aim, however, will be to influence will. Effects fall into two broad categories: physical (often called kinetic), which can be targeted against capability, and cognitive, which can be targeted against will. They can be primary and subsequent (second, third, fourth order, etc), intended and unintended. Effects can be applied to friendly, adversary and neutral parties, across the seven dimensions of the strategic environment[12] by using each of the instruments of power[13]. To unlock the full potential of EBO, future commanders will need to exploit a much richer information environment than hitherto. It is important to emphasize, however, that to achieve the desired effect in some circumstances it may still be necessary for British soldiers to 'take the bayonet to the Queen's enemies"as the only way of affecting an adversary's capability and will.

FUTURE ETHOS

Over-reliance on past lessons can lead to the phenomenon of 'preparing for the last war', which is a high-risk strategy at a time of rapid geo-political and technological change. We propose a more balanced approach that recognizes the value of historical analysis but demands a forward-looking posture underpinned by an ethos of *agility, optimum tempo and persistence*.

Agility is a core ethos of mind, function, equipment and procedure. It will be fundamental to future operations and has four attributes, which can be measured: responsiveness, robustness, flexibility and adaptability. *Responsiveness* is the speed with which force elements recognize the need for action or change relative to an adversary and is, therefore, a measure of how quickly we can seize the initiative. We must assume that in future, when faced by an asymmetric threat, we may start from a position of disadvantage when speed will be critical if we are to regain the initiative. *Robustness* is not just the degree to which forces remain effective following degradation, but also the ability to conduct different missions with the same capability. We can no longer afford 'single note' instruments (ie, dedicated organic capabilities). *Flexibility* is the ability to operate along multiple paths and present an adversary with complex and unpredictable futures. It also seeks to avoid the trap of foreclosing options at too early a stage in planning. In addition, it will allow us to overcome system failure or enemy action by ensuring we are not dependent on a single course of action or only one way of operating. Most importantly of all, *adaptability* is the aptitude of force elements to learn rapidly about their operating environment, particularly when faced with the unexpected, to recognize the need for change[14] and then reconfigure to succeed. Whilst agility describes notions of speed of reaction, or even pro-action, it need not substitute speed for mass. Indeed, agility can be exploited to achieve mass from a dispersed force, if that is deemed desirable, for example to mask blue force intentions.

> Agility will allow us to counter the unexpected with more confidence

Commanders will seek to achieve and maintain *decision superiority*[15] at all levels to gain and retain the initiative. Better SSA will be a major contribution to decision superiority but also requires more responsive and adaptive command processes, to improve the decision-action cycle and deliver decisive operational advantage in the form of enhanced *tempo*. Tempo is the rate or rhythm of activity relative to an opponent; higher tempo allows a commander to get inside the adversary's decision-action cycle by exploiting information and acting on it before the adversary has time to react. Tempo must, however, always be viewed as 'speed within context'; in certain operating environments, we may wish to pick the correct time to act, and timing can be more important than time *per se*. We shall require commanders who have an intuitive 'feel' for the precise moment when they have sufficient information to take or seize the initiative, without waiting too long and losing it. Finally, tempo allows the sudden massing of effects to achieve surprise. In a highly networked force, where the tactical level of command is fully empowered, a high degree of synchronization may manifest itself as 'swarming'. These natural opportunities for simultaneity, whereby an adversary is overwhelmed by threats so that he is unable to concentrate on any one, or even establish priorities, are key to achieving operational momentum and to shattering an adversary's cohesion. The overall effect of tempo is reinforced by *persistence*, an ability to maintain effects over time, should this prove necessary.

Optimum tempo will shatter an enemy's cohesion in warfighting and ensure effects are delivered in the best sequence in other operations

COMMAND

The authority for the direction, coordination and control of joint and integrated forces[16]

SSA, together with widely shared command intent[17] should allow forces to grasp and generate fleeting opportunities, and to cross traditional environmental (land, sea, air) and functional boundaries (intelligence, operations, logistics, etc), confident that it will not lead to unintended effects such as fratricide and collateral damage. The result should be an ability to create effects at optimum tempo. There is tension, however, on the one hand with the responsiveness, creativity and freedom of action that the concept of agility seeks to enable and, on the other hand, the degree of control required to ensure tactical actions are harmonized with the required effects at the operational and strategic levels. We should strike the balance between the two by empowering all levels of command, but allowing higher commanders to 'reach forward' and exert control when appropriate - in other words, an 'adaptive' C2 system. There is a danger, however, that the continual oversight that networks provide can allow senior commanders, politicians and even their advisors to exercise detailed control on an almost minute-by-minute basis. This can emasculate subordinate commanders, lead to a reluctance to take risks or to innovate, and encourage a tendency to 'interfere-forward'. It will require high quality leadership to ensure that this does not happen and that subordinates feel free to exercise freedom of action. If we get it right, it will, however, be an expression of *mission command*[18] for the information age.

It follows that, in all operations, commanders will need to strike an appropriate balance between centralized and decentralized operations, also to ensure that they maintain clear lines of responsibility. The key to resolving the tension between the two will be a shared information environment that uses a richer, more broadly distributed and better understood *command intent*. This will set the conditions for both information flow and individual action. *Collaborative planning* will allow command intent to be engineered concurrently, allowing all force elements to understand the strategic context but to be focused on the operational or tactical commander's intent. SSA should allow *optimum synchronization*[19] between force elements but, if it slips, higher level commanders must be ready to reassert control. The ideal will be minimal corrections on the 'command tiller' to re-establish synchronization, followed by re-delegation to the lowest possible level. Although difficult to achieve (doubly so in coalition operations, where cultures and command philosophies differ), the prize is higher tempo and improved agility. Future training must address the tension between centralized and decentralized modes. For the bulk of force elements, particularly at the tactical level, the decentralized mode is the more challenging. At higher levels, training should emphasize the identification of those occasions where reversion to the centralized mode is appropriate.

The role of understanding

An operational environment that emphasizes agility and tempo will require commanders who have the confidence and flexibility to exploit fleeting opportunities, and who allow subordinates the freedom of action to use their initiative. Above all, commanders will need what Frederick the Great termed 'coup d'oeil' - the inner light of understanding derived from experience and intuition that will allow them to make sense of a chaotic, non-linear, battlespace. They will not only need to understand this environment, they will need to be comfortable in it.

Collaborative planning and execution

A shared information environment will allow commanders and staffs at all levels and functions to interact immediately a plan is initiated, and so to plan collaboratively. This is very different from the traditional approach, where multi-disciplinary teams at each level of command develop plans sequentially and then cascade orders downwards. First, because everyone is continuously aware of the strategic and operational level context, collaborative planning will be an important element of SSA. Secondly, it should allow much earlier identification of critical paths such as logistics. Thirdly, since force elements are privy to the same information as higher HQs, they should be more likely to respond correctly to fleeting opportunities. Lastly, it should reduce the time required to synchronize operations. Force elements may even be able to prepare for operations before being ordered to do so and plan on the move, as already demonstrated in US experimentation. Subordinate HQs at every level should be able to initiate their part in the operation, with SSA allowing continual adjustment and coordination across virtual flanks[20].

Collaborative planning will be a key element of SSA

Networked information will allow force elements to remain dispersed for as long as possible, which will enhance force protection and minimize logistic footprints. As mission planning evolves, force elements would assemble virtually, Force elements will be mission and not environmentally organised. C2 structures will be more responsive.

across component and echelon, to form *agile mission groups*, coming together physically only at critical junctures, to maximize concentration of force whilst achieving economy of effort. The composition of mission groups would vary according to the specific capabilities required and the scale and duration of the task. This virtual assembling could also mask intent by providing unpredictable patterns of operation and increasing the likelihood of surprise. This concept would, however, have major implications for logistic support compared with traditional operations. The understanding of command intent by logistic commanders will be critical, as will be their own speed and freedom of manoeuvre. On the downside, the inability to interact in person and for commanders to exercise their physical presence may erode mutual trust and cohesion, and it will be essential to maintain formed teams at certain levels of command. Unit integrity and mutual trust are critical to making mission command work at the tactical level and must not be sacrificed in a headlong rush for agility.

Staff organization must also become more agile. The availability of information on a network should erode the tendency to stovepipe information within traditional staff branches. Smaller HQs would help cross-fertilization and it may be that the traditional J1-J9 staff branches are no longer appropriate. Future HQ structures could, for example, extend the current PJHQ philosophy of adopting task-oriented planning and execution groups, who take ownership of operations from inception to completion.

Coalition C2

Coalition warfare will require us to work with a wide range of capabilities and cultures. Cross-component and coalition C2 should be viewed as a requirement to initiate and coordinate tasks[21]. Technological capability, along with these human and organizational attributes, can be used to describe the need, first, to *integrate*[22] for combat operations with key allies who are able to exploit the future information environment, but perhaps only *inter-operate*[23] with other multi-national (MN) forces. In the extreme case of allies with no digitized capability or strong cultural barriers, we shall *de-conflict* entirely, although we shall still seek unity of purpose. Integrated forces will exchange near real-time information over secure links using shared procedures, a common command ethos and deep understanding of cultural differences. Inter-operable forces are likely to use reversionary techniques and processes such as liaison officers and standing procedures. De-conflicted forces will share a unity of purpose within the coalition but separate their activities in space and time to prevent them becoming an unacceptable drag on coalition tempo.

In most cases, it is the organizational, doctrinal and cultural aspects, not just the technological issues, that are the real barriers to interoperability. Of all these, security is probably pre-eminent. It, more than anything else, inhibits the flow of information within the military, between government departments and within a coalition. Differences between coalition partners will continue to cause friction. In particular, the British way of command may sit uneasily with the preference amongst others for more detailed control. The key will be to retain unity of coalition effort, if not the traditional view of unity of command. It is likely that some allies, even if they have the technology, will have cultural differences that inhibit the desired tempo. It follows that UK Armed Forces will require commanders and staffs who have the patience, tact, flexibility and cultural empathy needed to minimize these difficulties. These qualities will also be required for managing relations with non co-operative agencies, such as NGOs, who can create both positive and negative effects.

It is the organizational, doctrinal and cultural aspects that are the real barriers to interoperability

Control

Control is about guiding an operation; ideally, commanders will exercise a degree of control consistent with the objectives at their level. Command should, however, be de-coupled from control wherever possible because control of forces consumes time and may hinder rather than help tempo. Put another way, the objective of control is to contribute, not to interfere. Therefore the exploitation of technology to 'reach forward' is valuable only if it contributes to success. The imperfect interpretation of command intent[24], combined with chaos in the physical domain, may lead to operations becoming desynchronized and, therefore, the need for a measure of control to realign tactical actions with strategic and operational-level goals.

The control of forces consumes time. The objective of control is to contribute, not to interfere.

There are strong links between the complexity of the operating environment, what constitutes optimum tempo for that environment and how much control might be exerted to achieve it, as demonstrated by the way Army C2 has developed in Northern Ireland over the years[25]. Campaign effectiveness analysis is a crucial element of control. It is what allows commanders to detect discontinuities, adverse outcomes or simply the wrong effects occurring in the battlespace. With that immediate feedback, control can be exerted to shape the correct outcome.

INFORM

The acquisition, collation, processing, management and distribution of information[26]

Most of our current information systems are compartmentalized by component, sub-component, echelon and weapon system. Although recognized maritime and air pictures exist, and can currently be merged into a nascent Common Operational Picture (COP)[27], a recognised land picture is some way off. Therefore, a truly *joint* operational picture is a distant aspiration and, as a result, UK Armed Forces do not yet enjoy SSA.

In addition to SSA, 'Inform' is required to enable EBO by enhancing the information currently available (such as infrastructure nodal analysis, military capability and environmental data), and also to give more detailed knowledge covering culture, value sets[28], leadership structure, and the information needed for CEA, for red, white and blue components in the battlespace.

A new information paradigm[29]

Theoretically, SSA would give every platform and individual access to all information. The laws of physics and finance suggest, however, that this is not achievable whilst the information management challenge presented by our current level of digitization suggests that it may not even be desirable. Instead, we need a structured environment where sufficient information for comprehensive SSA is made available to those who need it. Above all, the current information 'push' paradigm, where producers determine what users need, should be replaced by an information 'post and pull' paradigm, where users state the requirement or extract what they need from 'bulletin boards'. This has enormous cultural implications, particularly for communities who have traditionally released information as they saw fit.

Communities of Interest

The detail of SSA required will vary at each level of command and a single picture will not satisfy all. It follows that the battlespace should be configured for efficient information sharing by identifying *Communities of Interest* (CoI), within which information flows can be matched to reflect the differing perspectives of commanders and staffs, as well as their capacity to handle information. It should also permit access to wider communities on demand, with information communities reconfiguring as required. Although 'pull' will be dominant, we should also have a culture that encourages all entities in the battlespace to 'push' information intelligently where they perceive a need elsewhere.

Of primary importance is that information communities are dynamic and not constrained by echelon, component or functional boundaries. Whilst this may seem a prescription for anarchy, experimentation shows that communities rapidly coalesce and adapt as operations develop[30], even if full freedom is given at the outset. To inform EBO, CoI must reach into the instruments of power and the information domains of coalition partners, OGDs and, when appropriate, NGOs. Examples of CoI could include: military strategic-level planners, task groups formed to undertake a particular line of operation and high data rate, pre-configured sensor-shooter groups.

> The information domain should consist of predetermined and reconfigurable Communities of Interest

Organizing ISR

To achieve decision superiority, commanders will need to secure information ahead of adversaries. An information position, however, is time and space sensitive, and should not be considered permanent or enduring. It follows that we shall need to focus our information-gathering resources at the time and place of our choosing and that we shall need an Intelligence Surveillance and Reconnaissance (ISR) management process to ensure that this happens and that high value assets are used effectively, even with conflicting priorities.

> All information has potential relevance at all levels of command. The notion of organic ISR will apply less in future.

The UK is unlikely to afford a collection system capable of permanent watch on a global scale.

> *'We cannot be all-seeing all the time –we simply do not have the resources"* [31].

It is, however, within our means to exploit a wide range of sources (military, diplomatic, allied, media) to provide indicators and warnings (I&W) that can cue a narrower focus to give a more concentrated regional view[32]. This approach *could* result in the UK entering a crisis in a position of information weakness. In this case, an initial disadvantage could be offset by the creation of pre-populated knowledge bases for likely crisis areas and exploiting knowledge bases held by other sympathetic parties[33].

Information support to EBO

Compared with the coarse-grained I&W system, EBO will require much wider, richer information[34]. In particular, it will cover all dimensions of the strategic environment with an ability to analyse adversary value sets, strengths, vulnerabilities[35] and the physical environment[36] for a Joint Operational Area (JOA). Finally, EBO requires us to understand and track measures of effectiveness for CEA. The effects-based philosophy seeks to achieve cognitive effects, which are difficult to measure. We need, therefore, a better understanding of how events affect an adversary's mind, which will depend upon correctly identifying reliable secondary and tertiary indicators of behaviour.

Analysing information

Analysis is the task of converting data into useful information. The detailed information needed for EBO implies an increased amount of processing, because of the far higher number of information sources. It is imperative that it is analysed using common processes across the joint force, otherwise different interpretations could lead to the delivery of divergent effects. Some raw data will have immediate use, but some will require assessment by specialists to enrich it and to avoid being deceived by an adversary. This concurrent process will require careful management for the following reasons:

- Processing can destroy information. The producers of information cannot know all the uses to which it might be put or the significance of some details for particular organizations. This reinforces the 'post before processing' paradigm so that information is not lost through processing[37].

- It will be important to get information into wider CoIs early and it will no longer always be appropriate for specialists to release the product of their analysis as completed packages. Agility demands earlier and wider exposure of potentially useful information, for which we shall need better visualization techniques if we are to make sense of it.

- The formatting and indexing of this less structured information must be carefully managed if correlation is to be made between key items of information within a CoI. New KIM techniques may become critical enablers for the integration of information streams, although the most complex correlation will continue to be undertaken by experienced commanders.

Exploiting information

The initial composition of a CoI would be determined as a result of the EBP process; it would then be primed by an intelligent 'push' of information. This initial burst must contain command intent and other critical information needed to set the context for subsequent information flow and exploitation. The information required by a pre-determined CoI (eg, a dedicated sensor-shooter team), is likely to be well structured. For more flexible CoIs that have been created for a specific task, the priming package is, however, less likely to be complete and will generate a greater need to 'pull' information. This, in turn, could lead to adjustment of CoI composition. A CoI should also push any new information deemed useful for others back into the wider domain. This inward and outward flow of information will enable better synchronization of elements, an essential requirement for increased tempo. A further benefit of synchronization should be fewer information gaps; this will lead to fewer requests for information and allow bandwidth to be preserved for swift responses to the unexpected.

Disseminating information

The future information architecture must be joint, reliable, robust, secure, interoperable with other MN forces and integrated with digitized forces. It is likely to be federated, linking established and emergent CoIs in a common domain. If it is to benefit from rapid advances in technology and avoid early obsolescence, it needs to be based on commercially available protocols and standards[38]. Ideally, it would enable a real and non real time capability at formed unit level. The only restrictions on access to information should be on the basis of classification, sensitivity or granularity. Managing access will, however, be made more complex by the need to support EBO.

Content-based information security philosophies and technology will enable a single structured information domain[39], which is essential to a 'pull'-based information handling approach. This could permit 'virtual' collaborative planning, thus permitting dispersal within or beyond the theatre of operations. Moreover, the availability of *reachback* to major databases and functions in the UK should help to reduce deployed footprints. Databases will require careful management. Information formats will also need to make best use of available bandwidth, particularly at tactical levels where the bandwidth is narrowest and the rate of messaging highest. Paradoxically, this could require a return to the discipline of formal staff processes, which have been eroded by the advent of e-mail[40].

> Our determined and clear aspiration must be a single information domain

Maintaining information

Given the role of information in the EBO process, information assurance will be imperative to ensure its availability, integrity, authentication, confidentiality[41] and timeliness. The information domain will need careful protection of both its physical elements and the information it contains. This is a critical vulnerability that will be discussed in the 'protect' element of the HLOC. Apart from the need in a democracy to audit decision making, there will be an increasing need to provide information that is precise, timely and evidential for proving the legality of military action, particularly where pre-emptive self-defence is concerned. As the legitimacy of our decision making is determined by reference to information that is reasonably available to us, timely collation and dissemination have additional impetus. There will also be the need to produce evidence rapidly to rebut adverse or incorrect media assertions. As a result, we must maintain an audit trail of all information flows that lead to decisions.

SUMMARY

- The future battlespace will be complex and uncertain. Globalization has created conditions where effects are very closely coupled with multiple, possibly unintended, consequences. Proliferation of information and weapon technologies is expected to continue but tolerance to casualties and collateral damage will diminish. Legal imperatives will constrain our freedom to operate and this will give our adversaries an asymmetric advantage.

- EBO could realize the full potential of the manoeuvrist approach. Effects are physical and cognitive, primary and subsequent, intended and unintended. They can be applied to friendly, adversary and neutral parties, across the seven dimensions of the strategic environment using each of the instruments of power. EBO seeks to exploit the full lexicon of effects, therefore its full potential lies across a wide spectrum of operations.

- Future operations are as likely to be in *ad hoc* coalitions of the willing as they are to be with established allies. The technological capabilities of potential coalition partners will range from those who attempt to stay abreast of US transformation to those who cannot. In most cases, it is the organizational, doctrinal and cultural aspects, not just the technological issues, that are the barriers to interoperability. Therefore we shall need to *integrate* fully for warfighting with certain allies but perhaps only *inter-operate* with others. In the extreme case, we may need to *de-conflict* entirely in space and time from those allies who do not share communication structures, processes or culture. The key will then be to retain 'unity of purpose' within the coalition.

- UK operations will be underpinned by an ethos of agility. This core ethos is characterized by responsiveness, robustness, flexibility and, most critically, adaptability. It is an attitude of mind and a benchmark for future capabilities, structures and procedures that will better enable UK Armed Forces to deal with the unexpected.

- The immense power of new information tools may go to waste until we understand which relationships between command and control are most relevant to the information age. We should decouple command from control to exploit the new information tools. Control should only be exercised if it *contributes*.

- The command and inform goal is to enable effects based operations to guide highly responsive, mission-oriented force elements that exert synchronized freedom of action throughout the battlespace. It is underpinned by shared situational awareness, a condition where force elements achieve a common understanding of both the operational context and tactical situation. The net result will be a significant operational advantage through a step change in agility and tempo. The command core concept is an enduring vision of mission command relevant to the information age. It promotes high tempo through the creativity and initiative of well-informed subordinate commanders. It relies on a network-wide expression of command intent and a high degree of SSA. An adaptive C2 process will seek to reduce the inevitable tension between desired freedom of action and the synchronization of effects needed to align strategic and operational-level goals with tactical actions. The result will be an agile joint force fully empowered to exploit with resilience the most fleeting of opportunities in the battlespace. Linked to the idea is the delivery of decision superiority, generated by SSA within and between task-orientated communities of interest. It will exploit a federated information architecture to facilitate collaborative processes within a single information domain.

Endnotes

1 JDCC, Strategic Analysis Programme, Summary of Implications, Pilot Iteration.

2 The UK Joint Vision, JDCC, 15 June 2001.

3 Defined as the three environments of land, sea and air, plus time, the electro-magnetic spectrum and the computer generated dimension.

4 A current description of Al Q'aida as birds, which generally travel alone but come together to form a flock in response to 'swarming' stimuli, may indicate the shape of adversaries to come.

5 In his seminal work, "Summary of the Art of War", Jomini described the geometric battlefield with boundaries and positive control lines that has characterized land warfare in the industrial age from the time of Napoleon through to the present day. In particular, he stated the requirement for a base, an objective, lines of operation and lines of supply. It was never a very successful way of describing the maritime and air environments, and is ill suited to warfare in the information age.

6 "In one moment of time, our service members will be feeding and clothing displaced refugees - providing humanitarian assistance. In the next moment, they will be holding two warring tribes apart - peacekeeping. Finally, they will be fighting a highly lethal mid-intensity battle. All in the same day, all within three city blocks". Gen C C Krulak, Comdt USMC.

7 Thea Clark and Dr Terry Moon, Interoperability for Joint and Coalition Operations, ADF Journal No 151 Nov/Dec 01.

8 V Adm M Stanhope, DCINC FLEET, at the Fleet Study Period, Maritime Warfare Centre, 26 Nov 02.

9 "Linking sensors, decision makers and weapons systems so that information can be translated into synchronized and overwhelmingly rapid effects". D/CM(IS)2/1(106/02) dated 29 May 02.

10 Situational awareness is defined as "the understanding of the operational environment in the context of a commander's (or staff officer's) mission (or task)" - JWP 0-01.1.

11 An approach to operations in which shattering the enemy's overall cohesion and will to fight is paramount. It calls for an attitude of mind in which doing the unexpected, using initiative and seeking originality is combined with a ruthless determination to succeed. British Defence Doctrine, JWP 0-01, 2nd Edition.

12 Economic, political, military, legal, ethical and moral, cultural, physical –JDCC Strategic Analysis, Pilot Iteration.

13 Diplomatic, military and economic.

14 In other words, to avoid 'groupthink', a recognized situation in close-knit groups whereby challenging the 'truth' can be perceived as disloyal or disruptive.

15 The application of knowledge by commanders to make quality decisions directing assigned forces and harnessing additional support at the right time, such that they preserve operational flexibility and maintain the initiative in the battlespace. DG Info (CBM) working definition May 02.

16 Definitions are taken from the Defence Capability Framework D/JDCC/7/1, 13 Sep 02.

17 'Command intent' is a statement that focuses on the decisive elements of how a mission should be accomplished. It must be rich enough to convey intent but simple enough to be unambiguous. The key is to leave sufficient room for initiative and interpretation by individual commanders. Adapted from Network Centric Warfare - Developing and Leveraging Information Superiority. 2nd Edition Aug 99 p34. David S Alberts et al, DoD C4ISR Co-operative Research Programme.

18 A style of command that seeks to convey understanding to subordinates about the intentions of the higher commander and their place within his plan, enabling them to carry out missions with the maximum freedom of action and appropriate resources. Adapted from British Defence Doctrine, JWP 0-01, 2nd Edition.

19 Optimum synchronization not only includes time and space but is achieved when primary and secondary effects are being generated in harmony with command intent, in particular the strategic and operational goals.

20 The disruption caused by the fuel tanker strike in the UK during winter 2000 is an example of so-called 'self synchronization'. Lacking any national leadership or formal organization, but armed with a common intent to move the government on the fuel tax issue, and informed by mass media, telecom and the internet, disparate groups acted in concert to create havoc. This concept is not as revolutionary as some would claim. A 1930s German Army pamphlet stated "The emptiness of the battlefield requires fighters who think and act on their own and can analyse any situation and exploit it decisively and boldly". The German Army system demanded that, when necessary, the various arms should coordinate and act together without direction from above. In J Storr, A Command Philosophy for the Information Age. Ed D Potts, The Big Issue, SCSI No 45, Mar 02.

21 As described in the US DoD "Levels of Information Systems Interoperability" (LISI). This sees seven support layers for C2: *C2 frameworks*, which constrain and support processes, which in turn can be organizational, legal, philosophical, financial or conceptual in nature; *C2 processes* that identify key activities, individuals and groups and illustrate how the C2 organization works; *information management* that captures stores and retrieves information; and finally, *information technology* and *communications links*. The emphasis on the higher level of support (C2 frameworks and processes) is towards people. It

highlights again the importance of the human element of command. Further human sciences research may be needed to optimize the development of future C2 structures, processes and training, whereas 'pure' technology has more emphasis at the lower levels (IT and communications links). A development of the LISI model (by Thea Clark and Dr Terry Moon, in "Interoperability for Joint and Coalition Operations", ADF Journal No 151 Nov/Dec 01) derives levels of interoperability from four enabling attributes: *preparedness* considers what doctrine, experience and training enable organizations to work together; *understanding* asks what level of information and knowledge sharing exists and how it is used; *command style* addresses how roles and responsibilities are delegated or shared; and *ethos* determines the levels of trust, culture, values and goals that are shared.

22 'Combine or be combined with to form a whole'. Concise Oxford Dictionary, 10th Edition.

23 'Able to operate in conjunction'. Concise Oxford Dictionary, 10th edition.

24 There is a human factors' issue when conveying an experienced commander's thoughts to less experienced subordinates through the information domain, where the 'lens of human perception' can complicate the process. Whilst doctrine and training make the process more predictable, intent is often misinterpreted.

25 A good example of an 'adaptive C2' system that works well is UK Army operations in N Ireland, a very politically sensitive operating environment. Land forces in N Ireland have had an 'all informed' voice radio system for twenty years, whereby the GOC (if he chooses) or any other commander can listen to any tactical radio net. This has proved very powerful for media ops staff, for example, who can listen to an incident as it unfolds and issue a very rapid and credible account, before other organizations who may wish to give a different version of events. Although the GOC and brigade commanders could in theory 'interfere forward' on the tactical net, in the authors' experience this happens very rarely. Long experience has taught that this creates uncertainty and confusion at a time when tactical commanders have to think and act very fast indeed. In other words, it does not *contribute* to the success of the operation. Any corrective action tends to take place 'off line' between commanders and staffs, so that the integrity of the chain of command is maintained and not undermined.

26 Definitions are taken from the DCF.

27 The COP is a subset of the JOP that shows the current, near-real-time picture. The JOP is a much broader information tool. See 'Inform: Exploit' below for a full description of the COP and JOP.

28 Those 'values' held by an individual, group, organization, regime or nation, which form the basis of their strategic centre of gravity. This involves understanding a potential adversary's psychology, plus the formative factors (cultural, religious, ideological, historical, economical and political) that drive his intentions, objectives and modus operandi.

29 A technical example, pattern or model. Concise Oxford Dictionary, 10th Edition.

30 US experimental experience indicates that CoI self-configure very rapidly once information starts circulating around a network. Personal communication from Vice Admiral Cebrowski, Head of the US DoD Office of Transformation.

31 CDS Speech to RUSI, 10 Dec 01.

32 The 'cue-scan-focus' approach. Maj Gen R Fulton, UK MoD Capability Manager (Information Superiority) in a speech to the RUSI C4ISR Conference 10 Sep 02.

33 It is likely that soon most major NGOs, for example, will have accessible databases for areas where they operate. It is likely, also, that these knowledge bases will have been built up over many years and will represent a body of knowledge that the military could not hope to replicate in normal operational timeframes.

34 The elements of information 'width' or reach are: sharing by functional area; sharing by alliance/coalition; sharing by component/echelon; sharing latency; sharing by security level; sharing by number of nodes; continuity over time; and geographic range. The elements of information richness are: completeness; correctness; currency; accuracy or precision; consistency; assurance; timeliness; and relevance. P 95 - 100, Information Age Warfare, David S Alberts, John J Gartska, Richard E Hayes and David A Signori, DoD C4ISR Co-operative Research Programme, 2001.

35 The JDCC-led Potential Generic Adversary project has a well-advanced study examining the motivational and capabilities aspects of future adversaries.

36 Geophysical, hydrographic and meteorological data for forces' manoeuvre generally, propagation information for surveillance sensor tasking and weapon performance limitations.

37 Information Age Transformation, David S Alberts, DoD C4ISR Co-operative Research Programme, 2002.

38 It is industry's view that in future military orders will be such a small part of their overall business that, as they are reliant on large volume/small margin production, investment in 'bespoke' military standards will not be cost effective. RUSI C4ISTAR Conference 24 - 25 Sep 2002.

39 JFCOM presentation to NATO CDE Conference Oct 02.

40 It is useful to reflect that Army operational 'Staff Duties' originated to facilitate message transmission using Morse code on telegraph and, later, HF radio - in other words to make full use of restricted bandwidth.

41 JWP 3-80 dated Jun 02.

42 The authors are pleased to acknowledge the substantial and valued input to this annexe provided by David Hull, ISTAR Technical Capability Leader, Dstl and Dr David Ferbrache, DSc(M/IS).

43 The DTI have initiated a 3-year programme to harness and develop the capabilities of grid computing.

44 The US are proposing to use UAVs for targeting information in urban environment, a man-portable micro-UAV being sent up to find targets and direct fire from a ground vehicle that can launch weapons, directed to the target by the UAV. We shall need to consider a legal provision here - see article 57 of Additional Protocol 1, to which the UK is a state party while the US is not. It is possible that technological advances will need to drive changes in the law.

45 The back-scattered light from the target is mixed with the transmitted beam and the Doppler frequency arising from target motion can be extracted. This can be used to identify vehicle types at many kilometres range by listening to their vibration modes and engine note. Because of the small beam width, this sensing system needs accurate cueing to a specific target region.

JDCC, MoD Shrivenham, Swindon, Wiltshire SN6 8RF
jdcc-adconcepts@defence.mod.uk

Annexe A - Major science & technology thrusts[1]

This annex summarizes technology trends most closely associated with command and inform capabilities. We make no assumption about affordability or the outcome of investment decisions. Past commercial products were often spin-offs from defence but, whilst there are exceptions, the reverse is now true. Therefore the MoD will, in the main, be embracing hardware and software developments from civil rather than military-focused organizations. The MoD may need to configure itself to take advantage of the commercial sector short time to market. Key developments are as follows.

Entertainment, automotive and telecommunications industries

The entertainment industry has produced wide-band high-quality video storage and transmission, very high speed and quality image rendering (automatic abstraction of image 3-D structure and fast interpolation techniques) that will be the basis for some future data compression techniques. A current saloon car has about 70 embedded processors. Embedded computing raises issues about fault tolerance and EMP protection if the military follow this lead. Although there has been a downturn in the telecommunications industry, there is a still a major investment in highly capable mobile communications.

Bioinformatics

This is a relatively new application of computer technology to process, store and access data in support of the growing genome and life science projects.

Knowledge and information management

This is set to become a dominant, if not *the* dominant, technology issue. There will be a need to increase both the effectiveness and efficiency of sensor and other forms of information processing. Ways of filtering unwanted information are critical, and 'personalization technologies' and 'user cluster nodes' are but two of many initiatives that may reach relevant conclusions in the coming years. The major challenge for the technologists is to provide the analysis tools and the presentation of information in the most effective and efficient manner whilst not overloading the commander, the operators or the support staffs. The challenge is to gather, process, interpret, communicate and display the information in a manner that permits timely decisions to be taken, in some cases, automatically. But the adoption of automatic decision-making techniques will be subject to legal considerations before certain courses of action can legitimately be pursued. The law may constrain how far we can go, and different perceptions of constraints, even between the US and ourselves, may become a factor.

The commercial sector and parts of the military, especially in the US, are investing substantial effort into technologies that can store, analyse and disseminate huge volumes of electronic data. Technology thrusts include data mining, automatic data reduction/filtering and data compression (the data compression being especially important 'in the last mile', usually at the tactical level, when information leaves wide-band fibre and uses radio. Other developments are expected in data/information management across multiple databases. This will be especially important in the NEC era where database-to-database information transfer, systems management and information assurance will be undertaken by computers, not humans. This will be acceptable as long as we retain the ability to detect what has become unreliable, a requirement that stems from the legal obligation to ensure that attacks are discriminatory.

Human computer interfaces

Paradoxically, the increased use of autonomous systems places an increased emphasis and priority on the need for human science research. The commercial sector and the US DoD are developing technologies that will allow more direct and efficient human-computer interaction. Such developments include sophisticated visualization technologies such as 3D immersive, virtual and mixed reality systems, 3D volumetric and virtual retinal projection, the US Navy research at SPAWAR being especially impressive. Other developments will facilitate automatic speech generation, facial recognition, translation and interpretation.

Also in development is pervasive computing where sensors, control interfaces and 'intelligence' are embedded everywhere in the environment (buildings, artefacts and people). So-called 'plastic electronics' will enable computers to be moulded and formed into clothes and equipment at low cost, making wearable computers both practicable and cost-effective. The military impact of such systems could be to reduce operator loading (or permit other, higher priority stores to be carried). Such developments, along with the possibilities of implant technology and neural-electronic interfaces, suggest that we shall see a fundamental change in the way we interact with the computer over the next 20 years.

Computing

The performance of computers continues to develop rapidly. Increased computing power in processing and fusion will mean that human (and not machine) delays will be the critical path. Developments in the next 20 years could include nano-computing, the use of computer assurance with automatic code generation, a convergence of security and safety-critical technologies and standards.

Communications

More effort will be given to managing and controlling the spectrum, which will become a valuable and contested commodity. There will be an increased need for spectrum re-use, improved data compression and spread-spectrum systems. There is a growing difference between those organizations that are able to exploit such technologies and those that cannot. But future alliances will require MoD to be able to communicate with both. Current developments aim to deploy fibre cables in theatre (the bandwidth for fibre links is now approaching petabit rates), wide-band point-to-point links using adaptive and electronically steered antennae, the use of laser communications and increased use of UAV and satellite relays (large, small and micro), as part of a network system. Further developments will see the increased use of low probability of intercept radio and self-organizing wireless networks.

Data fusion and exploitation
Effective fusion techniques and tools will exploit data from multiple sensor systems, providing opportunities for cross-cueing and data fusion.

Data processing
It will become easier to find patterns in data and to spot exceptions and anomalies. Data and information management will help to improve the provision of relevant information to the decision-maker.

Information distribution and sharing
These technologies will reduce the time taken to find relevant information and should permit a greater proportion of the organization to see it. In this way the C&I vision of greater SSA will be delivered. Technologies like the semantic web will be helpful in delivering SSA, as will those technologies that aid collaborative working. Instant messaging technologies should reduce the time needed to initiate and control interaction.

Data mining
Organizations will put far more effort into extracting every last piece of data from databases. There will be a far greater drive towards tailored sales packages linked to consumer needs. This implies sophisticated data mining, relationship derivation and time series analysis tools, which can be used for intelligence purposes.

Visualization technologies and techniques
Visualization techniques have the potential to improve the perception of information. 3-D displays, for example, could give better understanding of time and space relationships for tasks such as airspace management. Their early promise, however, has been undermined somewhat by subsequent research that has found they are not as widely effective as they might at first appear.

Speech recognition and generation
Speech recognition already enables devices to be controlled effectively when hands are occupied. Speech control would reduce the need to be tied to a workstation but is not necessarily helpful for team-working or multi-tasking. Apart from device control, there are applications in intelligence for topic spotting in conversations and real-time language translation. Speech generation has the potential to reduce communications traffic, as information can be sent as text and then recreated as voice. Voice output from systems may allow more input to be handled at once – eg, voice warnings instead of messages displayed on screen.

Cryptography
Quantum cryptography will provide potentially unbreakable encryption. This has potential advantages and disadvantages: whilst our own information will be more secure, so will be that of potential opponents. Quantum cryptography has been demonstrated both theoretically and practically. Its virtue is that it includes public key cryptography, allowing key distribution to be made without it being possible to be unknowingly intercepted. Quantum cryptography requires a coherent transmission medium, and its best opportunities are in fibre-linked systems, where it has achieved ranges of about 50 km.

Next generation internet
Broadband wireless communications may become commonplace with deregulation of cryptographic protection. Techniques will allow better core security on the networks (protection up to application layer) but vulnerabilities will abound in sophisticated multi-media applications. There will be greater dependence on the internet and an increasingly aggressive regulatory and legal framework, but an equally increasing development of niche applications and communities.

Virtual private networks (VPNs)
VPNs have the potential to support agile mission groups, as they can be created relatively quickly and subscribers can be mobile. However, the industry development of VPNs is establishing the model for future secure community communications using protocols that have security vulnerabilities. Therefore the power and flexibility of civil communications may be lost to military users.

Grid computing
Grid or distributed computing provides consistent access to information resources and services irrespective of physical location or access point, analogous to the electric grid[2].

Next generation UAVs for multi-role operations
UCAVs will have C4I capabilities of requisite integrity. The potential roles for UAVs include surveillance, communications relay, targeting[3] and jamming. Systems will become increasingly capable of autonomous operations. Examples include a drive towards free flight in which UAVs, given basic information, can plan their own missions and self de-conflict with other assets. A key issue will be safety-critical and high-integrity software –our trust in such systems –as well as the treaty frameworks that may govern their operation. By 2020 we shall have sophisticated unmanned combat air vehicle (UCAV) systems, remotely controlled ground vehicles and unmanned underwater (and underground) (UUV) systems. The technology for autonomous operation will exist but rules of engagement may require a person in the loop operation. Pre-programmed systems such as the current cruise missiles will be replaced with systems that can be reprogrammed in flight to enable re-targeting or a change of role - for example, from a weapon to a surveillance system. Future mini and micro UAVs may use conformal sensor arrays and sensor information from different platforms to provide better resolution and coverage.

Space

The military use of space will be more significant, particular areas being the drive towards further deregulation of the commercial sensing domain (0.5 m resolution and below) and the use of technologies to produce cheap and readily deployed satellites tailored to specific tasks or operating as part of a large network of sensors. The US aim is to field a space-based radar constellation by 2020, with ground moving target indication capability, enhanced hyper-spectral sensing, plus missile warning and detection capabilities. Tactical applications are likely to remain limited by financial rather than technological constraints. The use of higher frequencies and wider bandwidths could improve resolution.

Sensors

Many of the current sensor technologies can be traced back to the World War II and the decades following it. Major breakthroughs have stemmed from improved materials, miniaturization of electronics, and rapid improvements in computing and signal processing. It is likely that these trends will continue but the greatest benefits are likely to come from the intelligent integration of sensor information. Miniaturization of sensors will continue, especially from the development of micro electro-mechanical systems (MEMS) technology. This would permit the design of micro-UAV systems, readily deployed unattended ground sensors, small sonar sensors, considerable reduction in power consumption, power and communication management technologies, and continued 'spin in' from the commercial sector in areas such as mmIC technology, with gearing from the next generation of personal communication systems. The general trend over the next few years will be to produce better performance sensors that provide the information faster at lower cost.

Radar

Sensors are expected to become more dominant as the requirements increasingly focus on all weather, day night capability against difficult targets (camouflaged, under trees, urban environment, decoys, etc). In the concept time frame out to 2020, phased array radars will become the main source of information, with digitization being possible at the element level. Conformal arrays will be used on unmanned vehicles and may be integrated into, or even form, the vehicle structure. Other developments will be: foliage penetration technology that should mature in 20 years; surface-mounted ground-penetrating radar, albeit with stand-off detection problems; moving target recognition and identification for ground targets; automatic target detection and recognition; improved resolution modes; analysis tools to interpret and present high-resolution data; and robust air target non co-operative target recognition.

Visible spectrum camera technology

The commercial market that will provide fully digital high-resolution cameras will dominate visible spectrum technology. Active imaging sensors will provide identification of vehicles at long ranges. Targets may be cued by radar or infra-red sensors and illuminated by narrow beamwidth lasers. Eye-safe lasers will be used with active imaging in burst illumination mode (with 3-D capability), obstacle avoidance and vibrometry[4]. Fast response high-resolution detector arrays and low cost diode-pumped lasers will be widely available. Mid-wave and long-wave infra-red detectors will continue the development from scanned to staring arrays. These will be widely deployable, uncooled systems being developed to take advantage of MEMS and nanotechnology. For the high performance end of the defence market, cooled arrays will still be required. Spectral sensing will be required across the visible and infra-red spectrum for detecting camouflaged targets and disturbed ground. Adaptive optics will correct for a wide range of atmospheric and climatic effects to maintain system performance.

Electronic support measures

The main requirements for ESM are in the areas of communications interception, radar specific emitter identification and precision location of emitters. Over the next 20 years, the use of the radio frequency spectrum will increase, and more sophisticated methods for signal extraction and source identification will be required. ESM systems will provide cueing for other sensors or weapon systems.

Unattended ground sensors

These will provide warning of activities and situation awareness, particularly in the urban environment. Sensors could be delivered remotely by artillery or UAVs (or it may be a micro-UAV that lands or perches). Technologies that may be used to detect people and vehicle movements are thermal motion, microphones, chemical, seismic, magnetic anomaly and ESM.

Mobile power supplies

The development of mobile power supplies has been slow. However, there are advances in lithium ion technology that will be practicable in the short term, with fuel cell technology promising much for the future. These silent and lightweight power sources will significantly improve mobility, comfort and concealment.

Survivability

There will be a need to design adaptable networks, which exhibit 'graceful degradation' and not critical single-point failures. The need is greatest at the system level - the network must be survivable. The key issue is whether to rely on large single points of vulnerability with sophisticated defences (eg, high value air assets such as ASTOR and E3D) or establish a large distributed network of relatively vulnerable (but inexpensive) sensors.

Increased adaptivity

There will be a greater emphasis on the ability of the 'system of systems' (or, more likely, the federation of systems) to adapt to the scenarios or environment it finds itself in. Examples range from: developing flexible plug and play C4I systems (allowing coalitions to be built), reconfigurable HCI (reflecting individual user needs and interaction profiles), sensor systems that are capable of dynamic reconfiguration to the environment and target sets (such as UAVs positioning themselves to fill surveillance gaps), and the use of adaptive beamforming and operating modes for multi-static sensors with sophisticated data fusion technologies. By 2020, we shall be able to design a headless system, or one in which each element of the system meets a range of separate requirements and can manage the contention for resources. These systems will be highly survivable as a result of minimizing single points of failure.

Increased precision

Sensors will increasingly be configured to detect and localize targets by signatures or characteristics. Examples are the use of spectral signatures in hyper-spectral sensing, acoustic signatures to recognize particular vehicle types, radar/comms modulations to fingerprint particular radars (and by inference platforms) and particular receivers. We may change our mindset fundamentally from surveillance of an area, to detect all potential targets, to surveillance of an area to localize only the targets of interest, moving the discrimination task from the operator and processing systems to the phenomenology domain.

Training

New approaches are being developed that will enable staff to cope with the new technologies in what some are calling chaordic (chaotic) environments. Developments include the use of auto-tutors, network-based reachback and mind sensors. The trend in the commercial world is to make devices easier to operate by using technology that is transparent to the user. Computer systems now come with ‘self-learning’ packages and new ways of interacting with computers are being developed for the games market. The challenge for defence is to follow a similar trend and aim for reduced training in the use of technology.

Endnotes

1 The authors acknowledge the substantial and valued input to this annexe provided by David Hull, ISTAR Technical Capability Leader, Dstl and Dr David Ferbrache, DSc(M/IS).

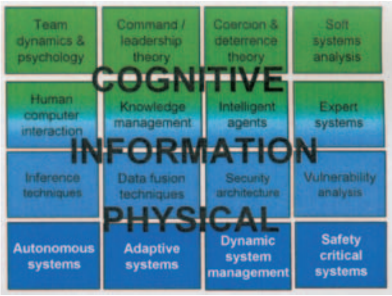
2 The DTI have initiated a 3-year programme to harness and develop the capabilities of grid computing.

3 The US are proposing to use UAVs for targeting information in urban environments, a man-portable micro-UAV being sent up to find targets and direct fire from a ground vehicle that can launch weapons, directed to the target by the UAV. We shall need to consider a legal provision here - see article 57 of Additional Protocol 1, to which the UK is a state party while the US is not. It is possible that technological advances will need to drive changes in the law.

4 The back-scattered light from the target is mixed with the transmitted beam and the Doppler frequency arising from target motion can be extracted. This can be used to identify vehicle types at many kilometres range by listening to their vibration modes and engine note. Because of the small beamwidth, this sensing system needs accurate cueing to a specific target region.

Network Enabled Capability: concepts and delivery - p 104

David Ferbrache



In recent years, several attempts have been made to provide a digital basis for battlefield functions and structures; none has achieved a commanding influence. NEC is different: while its essential components are digitally based, it is predominantly a philosophy in which the techniques are mere tools for providing a capability to collect, handle and distribute data, and which together enable battlefield management to be collectively informed, exceptionally flexible and aligned to a degree rarely experienced. In this introductory paper by one of the UK's leading proponents of NEC, the author prepares the ground for the theme papers that follow by reviewing some general questions about NEC, the answers to which will influence the rates of its acceptance, adoption and introduction.

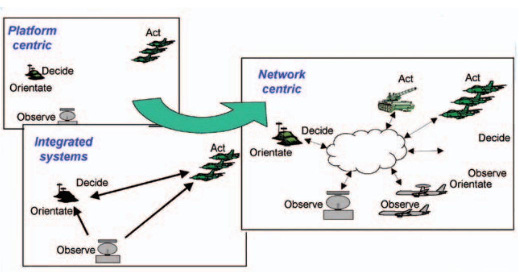
NEC is about improving network technology to facilitate radical changes in the way we structure and deliver defence capability. NEC can provide shared awareness, agility and synchronization: the first implies not only knowledge of dispositions but also of intent; the second refers to a capability for rapid reconfiguration; the third an unfamiliar harmony in execution. Already, the tools for effective networking are becoming available in the shape of sensors and communication systems. The challenge of NEC is first to explore how functions being procured against earlier backcloths can be harnessed and integrated to increase military capability. The solution is likely to include different methods of working, streamlined planning and execution processes, replacing traditional command hierarchies with empowered individual units, and throughout an underlying flexibility to reconfigure and restructure in response to operational circumstances. At all levels, getting value from NEC requires readiness to examine concepts of weapon usage, specification, development and procurement. The overall systems approach shifts the emphasis from seeking solutions to meet individual requirements to a high-level view of capability requirements. Successful evaluation calls for experimentation, real and synthetic. Application in turn will put new demands on training.

The effective introduction of NEC is unlikely to be baulked by insurmountable technical hurdles, though significant challenges lie ahead, particularly in information management from the most basic levels to the provision of the tools for a rich interactive environment. The greater need will be for a necessary shift in thought processes and methods of working, and for the communication of committed missionary zeal so that, from the back room to the front line, issues are instinctively thought of in NEC terms.

David Ferbrache is the Director of Analysis, Experimentation and Simulation in the Equipment Customer area of the Ministry of Defence. David joined RSRE Malvern some 12 years ago and has since been a DERA Fellow, Technical Director (Information Warfare), Assistant Director Technical Scrutiny (CIS), Deputy Director Intelligence Equipment Capability, and Director of Science (Manoeuvre/Information Superiority) on the central staff. His first degree was in computer science from Heriot-Watt University, and he has a Masters degree in business administration from the OU. He was awarded an OBE in the recent Afghanistan operational honours.

Network Enabled Capability –the concept - p 108

Anthony Alston



The MoD has stated that networked capability is to be central to the definition and operation of its future equipment capability. Implementing this initiative is called Network Enabled Capability (NEC); it is related to the principles of the US Network Centric Warfare programme. In UK terms, NEC encompasses the elements required to deliver controlled and precise military effect rapidly and reliably. At its heart are three elements: sensors (to gather information), a network (to fuse, communicate and exploit the information), and strike assets to deliver military effect. The key is the ability to collect, assemble and disseminate accurate, timely and relevant information faster to help to provide a common understanding among commanders at all levels. Research is being carried out to examine how implementing NEC affects the procurement of equipment. The author, a member of a joint project team led by Dstl, with support from QinetiQ and others, describes the initial findings.

The aspirations for NEC can only be achieved by changes across all the lines of development – in particular, in the equipment line, there is a clear need for coordination of platform and system definition, and acquisition. This will require hard decisions to be made regarding the balance between core capability, net ready (capabilities necessary for participating in a wider network community) and altruistic needs (those for the greater good of the network and beyond core requirements), without which a networked force cannot be achieved. The NEC conceptual framework derived in the paper provides a useful way of encapsulating the essence of what NEC is and what it is trying to achieve. However, to understand the impact of NEC fully, and its description in terms of the conceptual framework, requires stepping from the conceptual world into the practical one. This includes in particular understanding the impact on equipment acquisition and the metrics required to support it.

Anthony Alston of QinetiQ Ltd is a systems engineer with extensive experience in concepts for military information systems. He is supporting Dstl's NEC Delivery team.

Network Centric Warfare: current status and way ahead - p 117

David Alberts

Network Enabled Capability is known in the United States as Network Centric Warfare (NCW). This paper by one of the earliest proponents of the technique in the US is an informed, personal view of the present position and of what is necessary to ensure continued progress.

By its very nature, NCW is, and will continue to be, the product of many minds, and as such subject to many views and interpretations. However, at its most basic, it is the development and application of shared, networked, situational awareness to achieve better mission effectiveness between cooperating allies by true operational collaboration and a degree of self-synchronization. To be effective, this means that concepts of operation, organizations and approaches to command and control must evolve in parallel and in phase. Underlying satisfactory implementation is the implicit need for a willingness, indeed a commitment, to sharing and applying information, and immersion in a common philosophy. So, education and cultural change are root requirements for success. The author argues that the centre of gravity of warfighting capability moves from platforms to the network, perhaps surprisingly to the extent that the single greatest contributor to combat power is the network itself. Examples where NCW has been beneficial are mentioned, in one case with a reference to a particular example. But there is a long way to go: the point is made that the extent to which there is a common understanding of NCW theory and practice ranges widely, and that an agreed understanding is a requirement for the ultimate NCW experience. The immediate need is to move on from developing concepts and theories about network centric warfare to starting experiments in the field to test these ideas in practice. A willingness to provide significant funding will be proof of commitment to the ideas and the process. The author emphasizes the need for leadership to help the vision to be understood so that the required culture change can take place. A good starting point might be a demonstration at least of agreement between the English-speaking nations on what the approach should be called.

David Alberts is the Director, Research and Strategic Planning, OASD(NII), in the US Department of Defense. After receiving a Master's degree and Doctorate from the University of Pennsylvania, he has worked for more than 25 years on developing and introducing leading-edge technology into private and public service organizations *where he has held many senior positions while also establishing a distinguished academic career in computer science and operations research. He has published extensively in the open literature; his recent publications include the seminal books on network centric warfare and other aspects of conflict in the information age.*

Testing the impact of NEC options on communications infrastructure and campaign outcome - p 120

Lynda Sharp
Brian Stewart

Network Enabled Capability is in its infancy; at this stage, no-one knows how it will develop or how far its ramifications will penetrate. Much depends on the enthusiasm with which its philosophy and principles are accepted and supported. But, whatever its ultimate impact, and to have any effect at all, it will necessarily change the demands for information at all levels of command compared with the way military business is carried out now. This in turn will stimulate changes in the way headquarters are organized and in the processes followed for planning and conducting operations. Elements of ISTAR (intelligence, surveillance, target acquisition and reconnaissance) and the way they are networked – patterns of information flow around the battlespace and the information services required – will be particular candidates for change. To explore how these changes, the priorities and frequency of information exchanges, and the connectivity needed to share awareness, could affect communications infrastructure, a method has been developed to test whether programmed capabilities in information and communication services will be able to meet the demands of future military operations.

Effects have been addressed at two levels: first, at the communications network level, to examine the ability of planned networks to handle the demand for information arising from the conduct of future campaigns; secondly, at the campaign level, to compare the effects of investment in ICS and ISTAR with other investments in weapons and platforms. Both issues depend on an analysis of the flow of activity in a campaign and of determining the resultant demands for information. These demands are then tested against planned communications capabilities, and used to determine effects on campaign-level measures of effectiveness. The authors conclude that, while further work will be necessary, for example to track emerging NEC concepts, the analytical method can help to inform decision makers on both issues.

Lynda Sharp is an analyst in the Policy and Capability Studies department at Dstl Farnborough. She is the departmental lead on Information Superiority issues.

Brian Stewart is an analyst in the Policy and Capability Studies department at Dstl Farnborough. He trained as a physicist and generally works on ISTAR, ICS and campaign modelling related studies.

Quantifying the benefit of collaboration across an information network - p 123

James Moffat

Network Enabled Capability can be assessed from many aspects: the two particular studies described in this paper were concerned, first, with Theatre Ballistic Missile Defence, specifically, on the best way of defending deployed troops in theatre against ballistic missile attack, and secondly, with possible options for future headquarters structures.

Methods for defending troops against ballistic missile attack can range from deterrence to active and passive defence. The study focused on the place of counter-force in such a defensive mix and in particular on the development of quantifiable ways of measuring the overall benefit of sharing information to

Context and Synopsis

enhance the effectiveness of counter-force operations. The crucial factor in disrupting a missile attack is time because the window of opportunity is narrow; so the test to apply to a network of information is to determine the route through the network that maximizes the width of the time window. At the same time, sure knowledge is a measure of the benefit of collaboration, because it reduces uncertainty. Mathematical relationships are derived that enable information processing implications to be quantified to support a spreadsheet model.

Time is also a key factor affecting a measure of a headquarters' capability; but the quality of decisions is what ultimately counts. By combining the Rapid Planning Process representation of command decision making with Information Entropy as a measure of the knowledge available to the commander, a stepwise approach is proposed that allows for inconsistent evidence and information overload. The modelling captures the benefits of collaboration. The spreadsheet model will be applied in the first instance to the concrete example of a logistics problem where two brigades may or may not collaborate on fuel supply.

Professor James Moffat is a Dstl Senior Fellow, a Fellow of Operational Research and a visiting Professor at Cranfield University. At Edinburgh University, he took a first class honours degree, and was awarded the Napier medal in mathematics. He also holds a PhD in mathematics. After 20 or so years working mainly on defence-related operational analysis problems, his current research interests are in building tools, models and theories that capture the key effects of human decision making and other aspects of information age conflict. He was awarded the President's medal of the Operational Research Society in 2000. His most recent published works include the books 'Command and Control in the Information Age: Representing its Impact' (The Stationery Office, London, 2002) and 'Complexity Theory and Network Centric Warfare' (to be published by CCRP, Dept of Defense, USA).

The coalition agents experiment: network-enabled coalition operations - p 130

David Allsopp
Patrick Beautement
Michael Kirton
Jeffrey M Bradshaw
Niranjan Suri
Austin Tate
Mark Burstein

Major military campaigns increasingly involve multinational coalitions. From the time of the Tower of Babel (in what is now Iraq), where the main problem was language difficulties, the challenges facing coalitions have grown with the expansion of knowledge and the evolution of technology; these challenges now include data overload and information starvation, labour-intensive data collection and coordination, individual stand-alone systems, incompatible formats and scattered snapshots of the battlespace. Technical integration is not straightforward.

The purpose of Network Enabled Capability is to enhance military capability by exploiting information better. The Coalition Agents Experiment (CoAX) was an international collaborative research effort to examine how the emerging technologies of software agents and the semantic web could help to construct coherent command support systems for coalition operations. Starting with a rigorous statement of NEC core themes, the authors explain the basis of CoAX and how experiments were planned to ensure that the core themes were addressed by a few key objectives. A realistic and very rich coalition scenario was used for technology demonstrations, though the pressing problems of friendly fire and IFF were outside the scope of the research. The work showed how agents and associated technologies facilitated run-time interoperability across the coalition, responded well to unexpected battlespace events, and aided the selective sharing of information between coalition partners. Agent-based systems are adaptable and flexible in their demands on resources; they are not prescriptive, and do not override the commander's ability to act unpredictably, a major feature in wrong-footing the opposition. CoAX produced a prototype ‘Coalition agents starter pack” that could be developed further to support coalition warfare. In the round, CoAX was an admirable example of international collaboration at the research level demonstrating what, with the right tools, might be possible in a wider, albeit more pressing and tense, real-life context.

David Allsopp is a research scientist in Distributed Technology Group, QinetiQ. He has an MA in natural sciences and a PhD in materials science from the University of Cambridge.

Patrick Beautement is a principal scientist in the same group. He has a master’s degree in intelligent systems and was previously a squadron leader in the Royal Air Force.

Michael Kirton is a Fellow and is also in the same group. He has a BSc and PhD in physics from the University of Newcastle upon Tyne.

Jeffrey Bradshaw is a research scientist at the Institute for Human and Machine Cognition, University of West Florida. He received his PhD in cognitive science from the University of Washington.

Niranjan Suri is also a research scientist at the Institute for Human and Machine Cognition, University of West Florida, where he received his BS and MS degrees in computer science.

Austin Tate is a professor and technical director of the Artificial Intelligence Applications Institute at the University of Edinburgh. He has a PhD in machine intelligence from the University of Edinburgh.

Mark Burstein is the director of the Human Centred Systems Group at BBN. He has MS and PhD degrees in computer science from Yale University.

Many others participated in the work, which was supported by the MoD, DARPA and DSTO Australia. .

NEC social and organizational factors - p 142

John Holt

Network Enabled Capability behavioural and social research elsewhere has identified two major threads to the necessary development of shared understanding and implementation at the operational level. The first is based on understanding the thinking processes necessary to bridge the different viewpoints in a force using cognitive psychology; the second on understanding the cultural barriers to the acceptance of NEC, some of which are easy to overcome –by changing work processes and structure, for example – while others, such as deep-held beliefs about an organization, are more difficult. The present paper describes a third and in some ways intermediate set of social factors that influence building up effective working relationships. A set of factors is derived from civil practices, where digitized organizations, because they are often in competition, have to learn to share information with others to survive. Using data from reported social and organizational surveys, links between Network Centric Warfare (NCW) processes and social factors are derived. Key NCW processes that have been identified in earlier work include the degrees of shared information, sense-making, awareness and shared understanding. The quality of collaborative decisions and of interactions is used to reflect the decision-making process in the first instance. Some factors do not naturally fit into current NCW frameworks but are equally important – organizational climate is a good example. It is concluded that the social psychology perspective, which is based on building up trust between groups to foster working together effectively, could address some of the cultural barriers, while the organizational psychology viewpoint suggests that areas not currently covered under NEC research, such as organizational climate and organizational structure, must evolve to meet the demands of a stressful environment. The presence of social and cultural barriers presents a major test for those interested in developing network technology, as it may be difficult to tell whether shortfalls in the network are caused by technical or social factors. It is recommended that the presence of social factors should be checked by interviews with the different parties in a force. As a number of the social factors described are in other, non-defence environments, it would be useful to test their occurrence in realistic multinational force experiments and exercises. The measures suggested for building up trust in a force are potentially useful and their suitability should be assessed.

John Holt is a Principal Consultant with HVR Consulting Services Ltd, working on operational research and human factors. He graduated in behavioural science (1st Class Hons) from Aston University, gained an MSc in management science at Imperial College and a PhD in decision support in Naval C2 from Southampton University. He recently became a Fellow of the Operational Research Society.

Commanding Agile Mission Groups: a speculative model - p 152

Lt Col Merfyn Lloyd OBE RWF

Network Enabled Capability calls for a major revision of the way command is exercised in military operations. In the development of a conceptual framework for NEC, effects on command have been examined. Central to ways of improving operational effectiveness is the ability to deliver effects throughout the battlespace by the dynamic formation of agile mission groups (AMGs). An important step in considering the use cases is to consider how AMGs are to be used, how they form and how they are best commanded. The paper builds on the proposal of a functionally orientated command structure to develop a model for the command of AMGs to identify new ways of achieving improvements. The key to improving current processes is to share information and work collaboratively better. In terms of doctrine, the stage is set by the high-level operating concept determined by the parent Joint Doctrine and Concepts Centre. Using urban operations as an example, shared awareness and command intent are analysed, leading to the inference that the bounds on command intent are inherently flexible, to be adjusted as necessary to maintain synchronization with other AMGs and between the components of the commander's AMG. The decision-making process is outlined but not so rigidly as to exclude unexpected opportunities, always with an awareness of the lurking yardstick of the military measure of effectiveness against which achievement will be compared. This background need for flexibility feeds through to the functional command structure of the agile mission group and its necessary high level of shared awareness and command intent. The command management function derived meets the requirements of the high-level operating concept for agile forces, and in turn the aspirations of NEC.

Lt Col Merfyn Lloyd is the military member of the Dstl NEC Delivery team.

Can Network Enabled Capability be delivered? - p 160

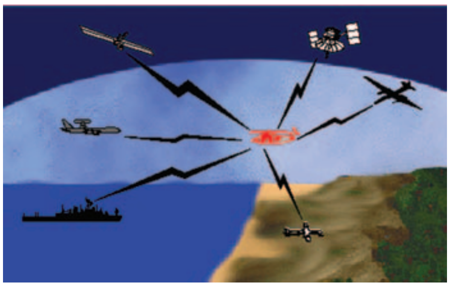
Richard Ellis

To improve the capability and effectiveness of UK forces by exploiting information better, which is the aim of Network Enabled Capability, it is necessary to identify not only those aspects of procedure and practice required to make NEC work but also how they are to be introduced. The author addresses this particular procurement issue, which, for the specific purposes of NEC, is termed ***inclusive flexible acquisition*** –defined as *coordinating processes across MoD, other government departments and industry that promote the rapid insertion of new technologies, facilitate coherence between acquisition programmes and provide an incremental approach to delivering 'net ready' platforms*. The challenge is substantial. ***Coordination and coherence*** and ***managing change*** are not so different from the established aspirations of the MoD's acquisition system. Indeed, there are few challenges in acquiring NEC (or indeed in NEC itself) that are completely new. However, the scope and depth of NEC bring many familiar problems into sharp focus, and make their effective resolution essential if the overall aspirations of NEC are to be realized. Each of the separate procurement projects involved will have its own prime objectives; many will have different customers; most will have different timescales. But NEC will require degrees of project interrelationship and interdependence that will not naturally be high priority. Risk will necessarily be increased. Lines of development –structure and processes, concepts and doctrine, equipment capability, personnel issues, and training and sustainment –will need to evolve together. Changes in technology, requirements, interoperability and commercial practices will have to be accommodated. Inevitably, there will be financial issues. In the absence of the intention to create a dedicated Integrated Project Team to deal with NEC as a prime task, there will be an unparalleled need for coordinating developments across the MoD, mechanisms for managing the technical and programme coherence between a wide range of acquisition projects, for managing and anticipating changes in requirements and technology, and overall for a more coherent programme management approach to equipment capability acquisition to provide a wider view of coordinated programmes of activity and to allow intervention in acquisition projects to achieve higher-level programme goals.

Richard Ellis is a Principal Consultant with Stratum Management Ltd. He has over 15 years experience of system acquisition management and for the last eighteen months has been supporting Dstl in the development of the NEC concept and, in particular, exploring acquisition and requirements management issues.

The impact of Network Enabled Capability on the ISTAR system performance envelope - p 164

Stuart Eves



A single sensor is not always sufficient to give confidence that an indicated detection is firm enough to justify follow-up action. Thus several different collocated sensors working together in harmony would be a requirement for a network-enabled ISTAR system of systems. Furthermore, they would have to be able to cue each other if they were to work together effectively. The most important system drivers for comparing different options from the UK's present ISTAR capability are cueing ability, the scope for data fusion, compliance with rules of engagement, and redundancy and robustness. The overall ISTAR performance envelope is being improved all the time as better capabilities are introduced. Furthermore, some account should also be taken of the capabilities of foreign ISTAR systems and their scope for enabling the UK's systems to be attacked. Against this background, some basic studies have been carried out to assess what would be possible and practicable, and the UK has started to develop a database from which the needs for better imagery capabilities can be established using simple yardsticks for determining the performance of a sensor system – the area that must be viewed, the timeliness with which data are provided and the quality of the information. It is unlikely that the UK will be able to afford to procure sufficient ISTAR to make it unnecessary to allocate resources to a prioritized subset of the total requirement. And sensors may well have different collection probabilities against a given target, so some selection will be necessary, striking a balance between providing multiple sensor coverage of the selected targets and avoiding the problem of data deluge. The precedents of nature are often helpful: of the half-dozen common sensors with which evolution has endowed man, most work best at short ranges; by analogy, perhaps three or more sensor systems would be best for target aquisition, with performance envelopes matching weapon system ranges. At longer ranges, man depends on two sensors, which is also suggestive. It is concluded therefore that, while collectors with overlapping performance envelopes will be required for a network-enabled ISTAR system, an analysis of the UK's requirements database will point the way to a system of systems.

Stuart Eves is a space systems analyst who currently works in Information Management Department at Dstl Farnborough, following tours in DEC(ISTAR) and the DIS. His primary research interest is making space-based surveillance an affordable option for the UK MoD, in which connection he is the 'Godfather' of the TOPSAT programme.

Lessons for NEC from previous information systems initiatives - p 168

Jonathan Williams
Gerald Foley

Several attempts have been made by the UK over the last decade to harness the power of information systems to improve military capability; many failed to run the course. While NEC is still under starter's orders, the authors' purpose is to examine why its predecessors failed, in the expectation that at least the hazards causing earlier fallers can be avoided.

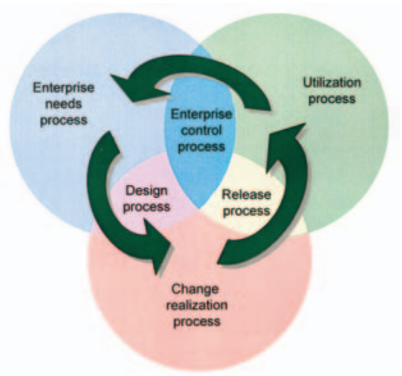
The starting point was the outcome of two workshops held earlier in 2003, and attended by all representative interests, to examine the reasons for earlier successes and failures. The MoD department responsible for determining and managing future capability requirements, which is keen to ensure that lessons from past experience are applied to the NEC initiative, supported the workshops. Conclusions were summarized under six headings: system scoping and analysis, where the lesson is to keep the main aim in focus and to avoid distractions by lesser issues; long-term financial planning to underpin future viability, an obvious necessity but one often ignored ; delivering capability, which for NEC entails bringing together discrete capabilities and systems for the benefit of the enterprise; programme management, a clear requirement that needs to be pitched at the right level; acquisition processes, which should be phased, flexible and accommodating; and technical management, where advantage might be taken of commercial standards and off-the-shelf solutions, with a leavening of operational experience. The transition from concept to implementation requires wide recognition that NEC is a new way of thinking about the problem space and becomes a way of life; its intent of networking decision-makers, sensors and weapon systems calls for wholehearted acceptance of the concept and commitment to the cause, and a full appreciation of the benefits, impacts and limitations at all levels. Lastly, but crucially, its implementation requires a properly resourced and empowered high-level 'champion' to make it happen.

Jonathan Williams is a Project Manager in Information Management Dept, Dstl. He has been associated with NEC since its inception in the research programme and has been instrumental in spearheading the rapid development of NEC concepts for the MoD.

Gerald Foley was the Technical Director, Systems in KI Systems Division, QinetiQ Ltd. He has contributed to the MoD's programmes on digitization and has held the technical lead for NEC. While in this role, he contributed to the present paper. He has now taken up an appointment in NITEworks.

NEC –the implications for acquisition - p 172

Peter Brook
Rob Stevens



Many authors in this serial of papers describe the technical aspects, implications, problems and requirements of NEC. At base, the core requirement is change – to methods of communications, to manifestations of command, and to systems integration at the battlespace level; above all, to acceptance of the concept, belief in its potential advantages and the will to make it work. To make it happen, no less a change will be necessary to acquisition, where many accumulated problems inevitably come home to roost, and to its overriding visibility in the wider context of the Enterprise business of the defence community. The authors describe in broad terms the changes to acquisition called for by NEC, and some of the work in progress on the novel underlying concepts. Though much has been achieved in recent years, legacy goes back a long way: in habits, methods of working, synchronization and phasing, integration, and processes and philosophy. Achieving integration at the Enterprise level is a particular difficulty owing, for example, to some incoherence in requirements, limited harmonization both between projects and component products, mechanisms for dealing with changes in operational activities and immediate needs, consequent effects on the management of procurement and possible contractual implications, and catering for uncertainty throughout the very long lives of major equipments, and their interfaces with each other and their environment, both operational and political. New processes at the Enterprise level are required to deal with these influences: some are in hand, others are in concept. A necessary step to enabling implementation has been establishing a MoD Integration Authority, of which the lead author is head. The IA is addressing architecture, processes and coherence, information management, modelling, and test and evaluation. A vision of the NEC world features large NEC programmes being coordinated into manageable groupings with many lines of development being run to a self-consistent pattern and managed under the overarching control of an Enterprise plan and conforming to an Enterprise architecture. Overall, the authors realistically recognize that the way ahead is necessarily uncertain and will not be without as yet unconsidered obstacles. Achieving success will hinge on the Enterprise culture entering the soul of the acquisition process.

Professor Peter Brook started with degrees in physics and spent his early career in microwave solid state devices and subsystems before transferring to the major systems area, since when he has managed a wide range of R&D programmes across the CIS and ISTAR domains. He was most recently DERA's Director of Systems Engineering before taking up his present appointment in 2000 as Head of the MoD's Integration Authority, based in DPA. He is a visiting Professor at RMCS Cranfield and was elected a fellow of the Royal Academy of Engineering in 1999.

Rob Stevens gained a first degree in physics and a PhD in solid state physics, and made early contributions in the fields of medical physics, satellite communications, signal processing and IT system design. He is currently the Technical Director of the IA where he is responsible for the technical coherence and technical architecture at the enterprise level.

The UK approach to future Command and Inform (C4ISR) - p 179

Paul Robinson
Lt Col Iain Pickard

The Cold War ended 14 years ago. Its demise removed the risk of armed conflict on a major scale but allowed lower intensity threats to take the world's stage, an opportunity that terrorists, rogue states and others bent on mayhem were quick to recognize, quicker indeed than defensive capabilities have been to react. The need now is for the structure, processes and equipment of the UK's Armed Forces to adjust to the new environment, to tune in to the new challenges, and to become lighter, more agile and mobile. The operational trend calls for flexibility, in the first place to enable effective coalitions to be formed as necessary and with whomsoever shares objectives and readiness on a particular issue, and, in the second, to be trained, prepared and motivated to deal with tasks ranging from peace-keeping and counter-terrorism to power projection and deliberate intervention. The response calls on the one hand for technological interoperability and on the other for a cultural shift to make joint or combined operations work. The key to the second is to exploit the tools provided by modern technology to redress the imbalance against adversaries unhampered by the constraints of civilized behaviour, while being mindful of the invasive capacity of information to overwhelm. The intention now is to adopt network enabled capability practices to link the tools of war with the practitioners so that information can be translated into synchronized and rapid effects. The authors discuss the shifting basis for future operations, the need for promoting the right ethos, and the effects on command and inform. An annexed check-list identifies some of the enabling technology trends most closely associated with command and inform capabilities. However, whether operational coalitions are fully integrated, inter-operational or separate, conclusions reached on a command core concept point to the overriding importance of a fully aligned sense of purpose to the ability of an empowered, agile force being able to exploit federated information effectively.

Paul Robinson was Assistant Director Science & Technology at the MoD's Joint Doctrine and Concepts Centre, responsible for the provision of scientific advice in the areas of planning, execution and assessment of effects-based operations. He has recently moved to a post in the British Embassy in Washington DC.

Lt Col Iain Pickard was on the military staff of the MoD's Joint Doctrine and Concepts Centre and is currently in Iraq.

Journal of Defence Science
Volume 8 Number 3 September 2003

Network Enabled Capability: