The Coalition Agents Experiment
A Prototype for Network-Enabled Coalition Capabilities

by **Patrick Beautement**

Patrick Beautement is a member of the Distributed Technology Group, QinetiQ Ltd, UK. Here he describes the Coalition Agents Experiment, an international research programme, which examined emerging technologies that might be used to construct coherent, flexible command support systems for coalition operations.

Nature of Coalition Operations

As recent events have shown, multi-national coalitions constitute an increasing proportion of military operations yet, despite our increasing familiarity with them, they continue to be a challenge. In addition to the problems of integrating single-service and Joint capabilities, the nature of coalition operations implies some need to rapidly configure diverse, incompatible, 'come-as-you-are' systems into a cohesive whole.

When coalition partners are familiar, doctrine, systems and procedures are aligned in advance. In reality, there are always uncertainties about exactly which capabilities will be provided by whom and about how the forces will be configured. Hence, coalition operations trigger the need for rapid, on-the-fly responses and cannot be predicated on using pre-existing co-ordinated systems – hence the need for flexible approaches that allow capabilities to be assembled at 'run time'.[1]

Relation to NEC

The overall aim of Network Enabled Capability (NEC) is to enhance military capability by exploiting information networks more effectively. The demands of coalition operations reflect the aspirations of NEC's Core Themes for flexibility, adaptability, robustness etc. NEC (and its US equivalent, Network-Centric Warfare) have been widely discussed [1, 2] elsewhere, yet their implications are not fully understood – especially in relation to acquisition. In essence, NEC is primarily a move away from the design-time specification and acquisition of fragmented capabilities towards the run-time composition and employment of complementary elements. Increasingly, this involves interoperability between NGOs, OGDs and commercial organisations – a very heterogeneous mix over which it is not possible to impose a single set of standards.

Diverse, open and distributed structures of this type are, de-facto, complex adaptive systems [3, 4], the boundaries of which cannot be rigidly delineated. Hence, it is impossible to fully define, at design-time, all possible states, configurations and interactions that could occur. This is both an indisputable fact and a major challenge as, if we cannot define it, how can we acquire it? Currently, the tool of choice is systems engineering, yet experience has shown that, especially when dealing with information systems, its use can lead to brittle, inflexible solutions. In extremis, these tools can unduly constrain the ability of commanders and their forces to act with agility and swiftness in response to unforeseen military imperatives.

So what is so different now that acquisition will be affected? In the last 15 years, information systems have become increasingly pervasive. So, as operational circumstances change in the real world then information systems at the boundaries of, and within, cyberspace must respond to these changes – but this has not been occurring. We have been able to achieve airspace superiority, for example, but we have not achieved the same in cyberspace. Hence, it is vital that we acquire capabilities which can act decisively, adapt at run-time and provide synchronised effects across all the domains shown in Figure 1.

CoAX: Brief Description

How do we go about achieving this coherence? Research carried out by the Coalition Agents Experiment (CoAX) between 1999 and 2002 has addressed

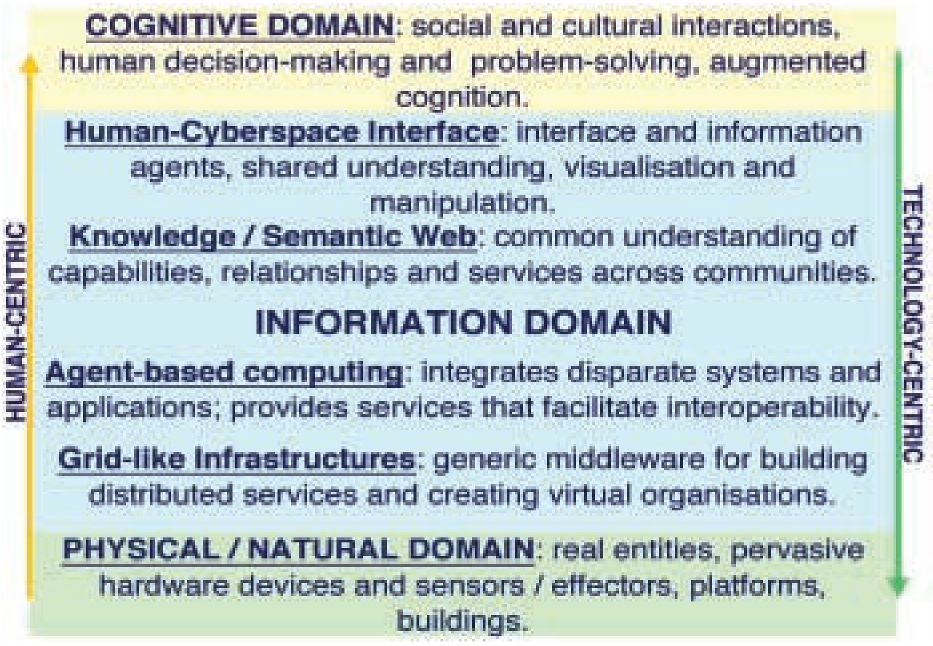

Figure 1. The mix of technologies required to achieve synchronised effects across all domains of distributed military enterprises.

many of these issues and can be seen as a de-risking exercise. CoAX was an international collaborative research effort which involved 26 military, academic and commercial partners, funded partly by the UK MoD, but primarily by the US Defense Advanced Research Projects Agency (through the $60M Control of Agent-Based Systems (CoABS) Programme [5]). The principal research hypothesis of CoAX was that emerging technologies such as software agents, information grids, the Semantic Web and agent control techniques could be used to construct coherent, flexible 'command support systems' for coalition operations.

A series of CoAX demonstrations was carried out between 2000 and 2002 using a modified Binni[2] scenario. The final demonstration was held in October 2002 at the US Naval Warfare Development Command, Rhode Island, before an audience of over one hundred senior officials from the US military, US Government agencies and UK MoD. These experiments showed how the use of agents and associated technologies facilitated the following:

- Flexible, timely interaction between different types of potentially incompatible systems, legacy applications and information 'objects' – leading to agile command and control and improved interoperability.
- The ease of composition, dynamic reconfiguration and proactive co-ordination of coalition entities – leading to adaptive responses to unexpected events at 'run-time', providing robustness in the face of uncertainty.
- The use of loosely coupled agent architectures, where behaviours and information are 'exposed' to the community, which is more efficient and effective than monolithic programmes.
- The use of agent policies and domain management enabling selective sharing of information between partners, leading to coherent operations, control of appropriate agent behaviour and an assured and secure agent computing environment.

CoAX produced a Coalition Agents Starter Pack[3] which could be extended and evaluated, for example, in future coalition warfare initiatives or within the UK's NEC research programme. Detailed information about CoAX can be found in the following references [6, 7], so I will only highlight relevant issues below.

CoAX: Technical Overview

CoAX started by embracing two principles. First, it took the open, heterogeneous, diverse and dispersed nature of the Coalition environment as a given – no single standard was mandated. Second, it put commanders in control, enabling them to acquire, visualise and manipulate diverse and dynamic information, however they wished it and whenever they needed it as the operational circumstances required. They were not required to define all this in advance. CoAX then put in place a range of technologies and tools which are summarised briefly below.

Software Agents. Agents can be viewed as semi-autonomous entities that help people cope with the complexities of working collaboratively in dispersed information environments. A community of agents works as a set of distributed, asynchronous processes communicating and sharing information by message passing. They work with users to make this information available whenever and wherever they need it, and can be organised to support individuals, military commands or virtual function teams [8]. Moreover, the agent paradigm provides the modularity and abstraction required for building large, distributed and complex active information networks [9] such as those required for NEC.

Grid Infrastructure. Agents and systems that are to be integrated in a Network-Enabled environment require infrastructures for the discovery of other agents and messaging between agents – such as the CoABS grid middleware which included an interface to register agents, advertise their capabilities, discover agents and send messages between them.

Control Policies. The increased intelligence that software agents provide is both a boon and a danger – agents can perform tasks

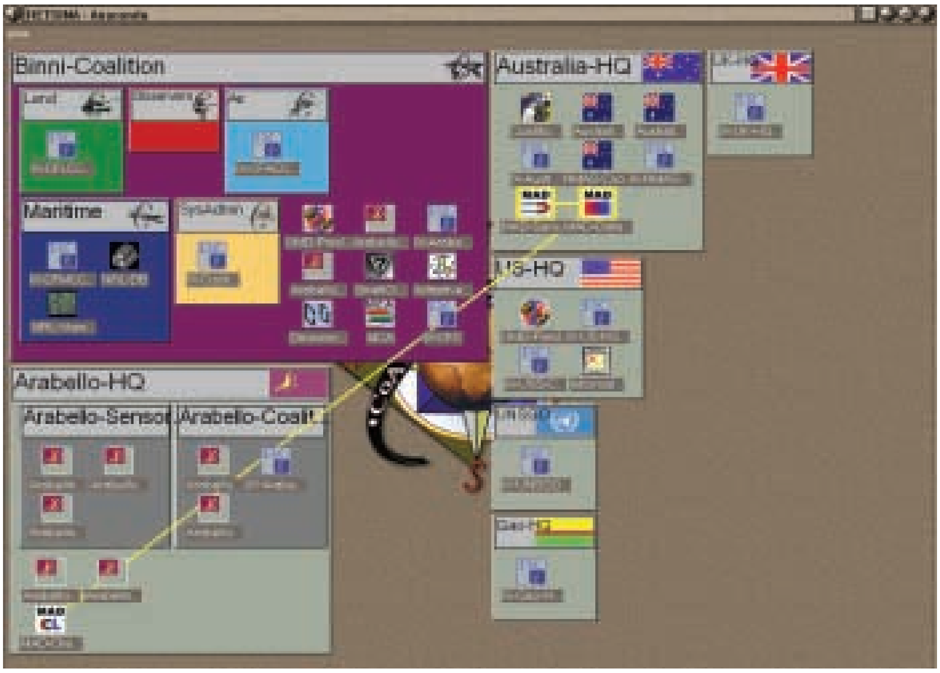

Figure 2. Agent Domain structure used in the CoAX Binni 2002 demonstration. Each domain contains a variety of agent. Domain nesting indicates a hierarchy of responsibility and control. Inter-agent activity can be visualised as part of full-spectrum dominance.

inside cyberspace that would be impractical or impossible using traditional software applications. However, this autonomy, if unchecked, could also severely impair military operations if buggy or malicious agents arose. In CoAX, the Knowledgeable Agent-Oriented System (KAoS) provided services to influence the run-time behaviour of agents from different developers and to running on diverse platforms [10]. KAoS services and tools permitted policy management within contexts established by complex military organisational structures. In addition, a system called NOMADS provided support for agent mobility, enabling capabilities to be deployed to where they were required at short notice.

Agent Domains. In addition, KAoS domain management services organised agents into logical domains corresponding to real-world organisational structures, administrative groups, and task-oriented teams – including allowance for complex hierarchical and overlapping structures. Domain managers administered agent registration and served as a point of administration for the specification, conflict resolution and enforcement of policies, represented in ontologies such as the DARPA Agent Mark-up Language (DAML) [11]. Figure 2 shows a typical domain configuration built on the CoABS grid and KAoS domain management services.

Semantic Web. Currently, tools such as Web pages are geared towards the visual presentation of information for humans, with no support for machine understanding, severely limiting the automated processing of information on the Web. The Semantic Web aims to have data on the Web defined and linked such that it can be used by machines for automation, integration, inference and re-use across various applications. 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, tasks and agent message content.

CoAX: Military Capability

The CoAX experiments demonstrated a range of military capability from information gathering in the planning phase through to time-critical targeting during execution. These experiments showed that CoAX supported the NEC Core Themes of dynamic collaborative working, agile mission groups, shared understanding, effects-synchronisation, full information accessibility and resilient information infrastructure. A brief snapshot of the military capabilities demonstrated by CoAX (and the roles played by the agents) is shown in Figure 3.

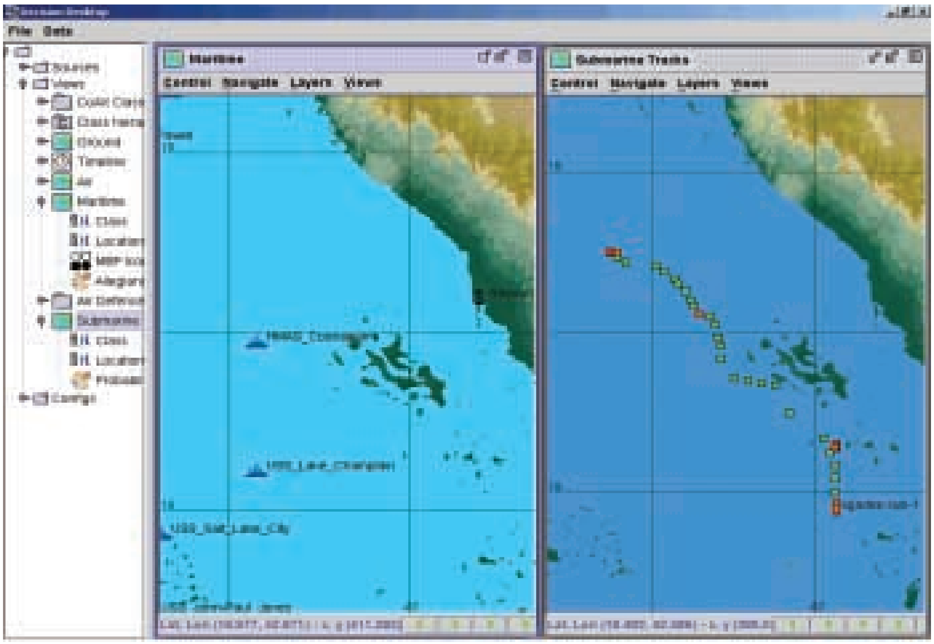

Figure 3. CoAX Binni 2002 – Submarine contacts from the underwater sensor grid are delivered to QinetiQ's Decision Desktop tool via the dynamic agent infrastructure. The rightmost panel shows that the commander has chosen to display them according to their confidence level.

CoAX Binni 2000. This scenario focused on the planning phase of conflict and 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, a new capability); the extraction and import of publicly available data on the Web; the detection and control of hostile agents; visualisation of the current state of operations and support for coalition shared awareness.

CoAX Binni 2001. The scenario for 2001 moved to the dynamic execution of operations, adding dynamic responses such as the integration of 'come as you are' agents into domains at short notice; further time-critical agent functionality (such as the de-confliction of Air Task Messages and updates exported from legacy battle management tools); run-time reconfiguration in response to changes in tasking and rules of engagement; and the integration and novel visualisation of remote, near-real-time sensor feeds with unclassified information from the Internet.

CoAX Binni 2002. The events of CoAX Binni 2002 followed on from those of 2000 and 2001, beginning with an attack on a monitoring ship in the Red Sea by enemy submarines. Interface agents worked collaboratively to report the attack, and the damage that was caused, by reconfiguring themselves to take account of information sources that were no longer available. Mixed initiative (human-agent interaction) messaging was used to request medical assistance. Mobile medical monitoring agents were dispatched and medical evacuation flights were de-conflicted as a result of agent-instigated alerting. Then a neighbouring country, prompted by the attack, offered anti-submarine capabilities. A Coalition

Agents Starter Pack was used to make selected parts of its underwater sensor grid capabilities visible to the Coalition by creating (on-the-fly) a 'go-between' agent that enabled intelligence agents to talk to a US fusion service. Agent policies were employed to control the dynamic filtering of sensitive information before passing it to partners. Using these techniques, information was published and was employed by the Coalition HQs to co-ordinate counter attacks. This process was driven by the decision-makers using the Semantic Web ontology-based tool called the Decision Desktop from QinetiQ [12], which provided information as and when they demanded it.

Pointers for Acquisition

In many ways, CoAX can be seen as a prototype of the kind of active information environment that could be acquired to support NEC. Information networks are usually seen as simple communication pipes between computers, but this is wrong. Cyberspace is an active battlespace to be dominated as part of Full-spectrum Dominance. Hence, it can be seen that new tools and techniques will be required, especially to enable co-ordination of effects across all battle spaces. Some initial pointers for acquisition can be drawn from CoAX, and these are presented below.

Reduce the Emphasis on Specifying Design-time Requirements. Acquiring agile information networks with the necessary capabilities requires an approach which goes away from specifying everything in advance. In addition, we should look at making the design-time properties of our devices such that they can communicate, be assembled into more complex systems and then be reconfigured dynamically at run-time. It has been shown that minimising design-time assumptions enables greater run-time flexibility.

Understand How to Employ Tools in the Run-time Environment. Some uncertainties can only be dealt with at run-time. Acquisition will need to provide tools which can alter run-time behaviour on-the-fly to meet the changing demands as operations are executed. In addition, we need to understand better how to exploit the phenomena which arise from these complex environments as force multipliers – for example, evolving and deploying emergent phenomena (such as a cascade of denial of service attacks) against an opponent rather than suppressing them [13].

Embrace Heterogeneity and Complexity – Not Constraining Standards. CoAX accepted the reality of coalition operations – that it is not possible to mandate a single standard – and showed that this was a strength which led to greater flexibility, security and robustness. CoAX identified that some standards could be seen as constraining and others as enabling (as they can be used as building blocks) and explored the possibilities for active interoperability negotiation at run-time – a different approach from the usual acquisition of tools with pre-defined information exchange requirements.

Exploit a Mix of Novel Architectures. CoAX showed how, within security constraints, shared information pools can easily be created by employing publish and subscribe mechanisms within a service-based architecture. In addition, legacy systems can be integrated if they are agent-enabled (exposing interfaces and data) – leading to better coalition-wide shared understanding. These information pools arise dynamically at run-time and are very robust – they are not, however, database applications procured in the conventional sense.

Conclusions

NEC aspires to improve military effectiveness by flexibly and adaptively exploiting networks of information in the battlespace in near-real-time, including coping with the unexpected. The 'come as you are' situations of coalition operations are similar in their requirements. The CoAX series of demonstrations was a prototype of the kind of active information networks required to meet these aspirations. The run-time adaptable technologies employed in CoAX have different characteristics to the stovepipe monoliths acquired in the past and different acquisition strategies will need to be developed to deal with them. Nevertheless, it is inevitable that a mix of highly specified and highly predictable tools will exist alongside the more open, distributed and flexible networks of information services as each have their place in the information armoury of the future. ■

REFERENCES

1. Network Enabled Capability: http://www.mod.uk/issues/nec
2. Network-Centric Warfare: http://www.dod.mil/nii/NCW
3. Santa Fe Institute: http://www.santafe.edu/sfi/research/focus/networkDynamics/index.html
4. Complexity Science – Network of Excellence: http://www.complexityscience.org/
5. *The Coalition Agents Experiment: Network-enabled Coalition Operations*, M Kirton et al. In Journal of Defence Science (Special edition on NEC), Vol 8, No 3, Sep 2003.
6. Control of Agent-Based Systems Web site: http://coabs.globalinfotek.com.
7. Coalition Agents Experiment Web site: http://www.aiai.ed.ac.uk/project/coax.
8. *Software Agents for the Warfighter. ITAC Consortium Report*. Bradshaw, J M, Boy, G, Durfee, E, Gruninger, M, Hexmoor, H, Suri, N, Tambe, M, Uschold, M, and Vitek, J., eds. 2002, Cambridge, Massachusetts, AAAI Press/The MIT Press.
9. *An Agent-based Approach for Building Complex Software Systems*. Jennings, N R. 2001, Communications of the ACM, 44:4, 35-41.
10. *KAoS: Toward an industrial-strength open agent architecture*, Bradshaw, J M, Dutfield, S, Benoit, P, and Woolley, J D. 1997, in Software Agents, AAAI Press / MIT Press, Cambridge, Massachusetts, editor J M Bradshaw. Pages 375-418.
11. *Making Agents Acceptable to People,* Bradshaw et al, in Intelligent Technologies for Information Analysis, N. Zhong and J. Liu (eds.), Springer 2004.
12. Decision Desktop. See: http://www.aiai.ed.ac.uk/project/coax/presentation/posters-29oct02/2002-qinetiq.ppt.
13. *Network-Centric Security – Approaches to Collective Run-Time Adaptation*, P Beautement, Adaptive and Resilient Computing Security Workshop, Santa Fe Institute, Nov 2003.

NOTES

1. In this sense, design-time activities relate to acquisition etc, whereas run-time configuration takes place during and after deployment and provides, therefore, the ability to flexibly adapt to the changing military imperatives of each unique operation as they occur.
2. Binni is a realistic military scenario (see http://www.binni.org/) developed for The Technical Co-operation Programme. It is set in 2012 and involves the UN in a conflict between two countries where WMD are an issue.
3. Coalition Agents Starter Pack available at: http://www.aiai.ed.ac.uk/project/coax/demo/2002/coalition-starter-pack.html