11th ICCRTS COALITION COMMAND AND CONTROL IN THE NETWORKED ERA		
Title: **"Agile and Adaptive Coalition Operations - Leveraging the Power of Complex Environments"**		
Topic: Coalition Interoperability, C2 Architecture, C2 Concepts and Organisations		
Author 1 (POC):	**Author 2:**	**Author 3:**
Patrick Beautement		
QinetiQ plc		
AT119, Malvern Technology Centre		
St Andrew's Road, Malvern		
WR14 3PS, United Kingdom		
Tel: +44 (0) 1684 896057		
E-mail: pbeautement@QinetiQ.com		

This paper is part of a set being offered by Dstl and QinetiQ which discuss topics of current interest. Each paper stands on its own though common themes connect them.

ABSTRACT

All life is a competition for the control and use of resources and the world of military endeavour is no different in this respect. That competition takes place an environment - our world - which is complex. This paper characterises some of the challenges posed and offers strategies for not only making those challenges tractable but also for turning them to advantage. Throughout the worlds of the military, commerce and government and in everyday life we are increasingly connected through complex networks of relationships and interactions, which can be represented at different levels of abstraction. For coalition organisations, the key word is agility - being able to adapt to the uncertainties of the world without dislocation, which is as applicable to the cyberspace that supports them as it is to the real world that they inhabit. They must be capable of engaging in continuous and innovative adjustment. This paper considers some of the mechanisms which can be exploited at design-time, assemble-time and run-time (DART) to enable this - influencing the structures and relationships in purposeful entities such as networked enterprises and ensuring the collective, adaptive and secure behaviour of entities in cyberspace. The focus of this paper is on how to cope with, and leverage, the complexities of the real world, at run-time, to achieve decisive advantage for coalitions.

INTRODUCTION

A major challenge faced by modern military and commercial enterprises is how to exploit, to advantage, the capabilities of the highly interconnected, heterogeneous, ever-changing and always-on complex environments in which they operate. New approaches are required to address this challenge. Traditionally, at 'design-time', we try to anticipate every possible circumstance and then design-in all the necessary features that we think may be required. Worse, we often design-in current processes and so risk 'freezing in' failed or outdated procedures. Then, at assemble-time, we carry out putative deployments to test the design against 'the specification', reverting to redesign if necessary. Though this approach has worked well with mechanical systems it is limited in its utility in complex network-centric contexts (such as where coalitions are facing insurgents) where highly adaptive and 'edge-like' agile entities operate. This is because it is impossible to conceive, in advance, of every possible situation and so, without run-time innovation and adaptation, we are condemned to operate within the limited set of options identified at design-time.

Hence, there is a need to identify and embrace run-time mechanisms and approaches which will enable us to adapt and restructure whatever is required on-the-fly during operations. One way to do this, as chosen in this paper, would be to review and characterise the notion of design-time, assemble-time and run-time and identify what can best be achieved in each situation. In essence we need to know what are the appropriate things to be doing when we design and acquire things; when we structure and deploy them and then what we should be doing when they are employed to leverage the dynamic power of complexity to decisive advantage. The paper will also characterise a range of run-time environments as these affect what can be achieved. This means shedding some of our preconceived ideas about boundaries (what is 'ours' or 'theirs') and seeing that the 'battlespace' is actually everywhere and that absolutely anything is potentially a weapon[1]. In addition, the paper will touch upon the equivalent mechanisms which will need to be at work in 'cyberspace'[2] and indicate how run-time behaviours in this virtual world might be harnessed to augment activities in the real world - enabling us to shape and adapt to the unexpected - an essential requirement if we are to succeed in modern military operations.

THE CHALLENGES OF COALITIONS

The military domain is a very challenging environment characterized by uncertainty including the need to be able to deal with significant and disruptive dynamic changes. Despite an increasing trend towards adopting approaches from the commercial domain, military activities are different in one key respect - there are opponents who are doing their best to aggressively frustrate or destroy friendly activities and assets and to deflect or subvert allies or neutral actors. This means that nothing can be relied upon and that therefore key capabilities of agility include: the ability to adapt to (or shape) change; to be innovative, flexible and responsive (and grasp fleeting opportunities) and to be robust and resilient (in the face of potentially catastrophic disruption). Anything that inhibits these capabilities is unacceptable.

These military activities are driven by human decision-makers who need support in making sense of the environment and with reasoning about, and effecting, possible futures. Conflict is, essentially, a human activity. Consequently, when supporting human-led endeavours such as military coalitions, the primacy of the human must always be kept at the forefront. The nature of

[1] In effect this takes the UK's 'Comprehensive Approach' (using all instruments of power in a coherent way: financial, diplomatic, military etc) to an extreme - which is what insurgents and terrorists already do.
[2] Can be thought of as "a notional environment in which electronic communication occurs between non-physical, and potentially purposeful, entities and devices".

coalition operations (a teaming of people from many backgrounds with various views of the world) implies the need to rapidly configure incompatible or foreign systems into a cohesive whole. Several key principles apply, that:

- the creation and maintenance of a cohesive coalition organisation (with real and virtual parts[3]) from the diverse and disparate 'come-as-you-are' elements provided by the coalition partners (people, processes and systems) is the key task which requires continuous, pro-active readjustment;
- multiple coalitions (and other entities) may be active at any one time ('competing' for resources etc) and a decision in one may affect another concurrent operation;
- partners may be part of a coalition - but their contributions may be anonymous (to protect sources etc);
- coalition elements should be supported by appropriate IT in achieving 'unity of action' and the systems provided must be robust, secure, dynamic and adaptable and must not unduly constrain human actions. In coalitions, cultural diversity should be embraced;
- "interoperability of the mind" is as important (for shared awareness and purpose), if not more so, than interoperability of systems. The difficulties are compounded in the virtual organisation of the coalition since there will be a mix of cultures, doctrines, equipment, operational procedures, languages, etc;
- most coalitions will have commercial / civilian elements - appropriate interoperability will have to be provided with their infrastructures;
- coalitions consist of loosely connected elements working semi-autonomously, and within their delegated authority, towards a shared purpose (as defined in the Commander's Intent). Elements need to rendezvous (and synchronise) only occasionally and must be free to optimise locally / snatch fleeting opportunities etc;
- supporting the achievement of command agility (working in a flexible, unpredictable manner - where the decision-maker is the only thing on the critical path - leading to supremacy over the opponent) is vital. This is especially so in the crucial (and often overlooked) part of conflict - that of Execution and Battle Management;
- enabling commanders to access relevant coalition-wide information (preferably as and when they demand it) to support their decision-making is crucially important to a successful outcome. Information should not be pushed according to some rigid, pre-determined process or design;
- there is a pressing need to be able to set up coalition organisations / systems rapidly (in order to respond decisively to emerging crises).

ISSUES ARISING FROM THE CHALLENGES

When reasoning about conflict one should always start by embracing the realization that nothing will be absolutely predictable and that being able to cope with uncertainty should be a fundamental aspiration. An aspect of this is the heterogeneity and complexity of the environment. Conflict with an opponent on a 'standardized' battle space will end up being an attrition war in some limited part of the conflict space. Instead, finding asymmetries (where you are strong and so can wield decisive advantage against an opponent) is an important manoeuverist strategy. This involves working with anything in the battle space which can be wielded as a weapon, including exploiting (even deliberately increasing) the complexity of the

[3] In other words, this paper is not just concerned with the physical world, but all worlds relating to human endeavour (physical, cyberspace, cognitive, social and cultural etc).

environment to undermine the opponent[4]. This includes cyberspace, which is a battlespace in its own right (not just a conduit for communication between people). It is a domain closed to humans and so 'cyberspace dominance' can only be obtained by using proxies to wield power on our behalf – such as software agents [1, 2, 3, 4]. The key is to always have available as big a range of options as possible (from which to generate novelty) as this is the counter to uncertainty.

Therefore, the challenges to be met come down to two main issues: having the structure and mechanisms to cope with or shape unanticipated or novel events in the wider environment, and: having the structures and mechanisms capable of operating in any type of threat environment (dispersed insurgents to defined enemy on a battlefield). For this paper, the key issues arising from the challenges are:

- acknowledging and characterising the way the world the works and understanding how it impacts operations - that the world, and human organisations, are complex and that, for success, this complexity must be mastered and turned to advantage;
- facing up to the limitations of the techniques and models usually employed in our business systems - that oversimplification has constrained what can be achieved;
- perceiving the options and opportunities which exist and which are, as yet, largely unexploited - by developing suitable toolsets and exploiting existing mechanisms;
- understanding how to embrace and positively exploit the complexities of the real world during operations - by using appropriate approaches and mechanisms to design, assemble and operate our military organisations and business systems.

NETWORKED, PURPOSEFUL ENTERPRISES

Our aim, therefore, should be to face up to these realities and always strive to create coalitions which operate as 'networked enterprises'[5]. Networked enterprises consist of organisations which are collaborative in that they are inclusive and flexible (as opposed to hierarchies that are authoritarian and exclusive). Because they recognise the need to cope with the uncertainties of the real world, they are agile and 'plastic' - able to combine and employ their elements on-the-fly in novel ways. They are also unconstrained - being able to adapt continuously to changing circumstances, including being able to cope with sudden opportunities, changes, dislocations or disruptions. Fundamentally, networked organizations can change their 'operational system'[6] [5] as needed to change or to exert influence in any domain where the organisation is in contact with other actors or the environment. Networked organisations should to be able to:

- sense their environment and behave as if they are self-aware (enabling them to evaluate, assess and continually adjust their purpose);
- be inherently unconstrained and not pre-optimised (they can cope with uncertainty and surprise as a matter of course);

[4] Interesting game theory analogies apply here - a known strategy when playing chess against a computer is for the human player to deliberately enter parts of the search space that are more complex, where the computer can't search very deeply. In Othello, a significant metric is "mobility" - the number of moves you have available compared to the number of moves available to your opponent.

[5] Where 'an enterprise' is actually a distributed community of elements such as commanders, operating units, strategic partners and service providers collaborating within sets of 'contractual' frameworks with multiple allegiances to other 'enterprises' and where relationships can change moment-to-moment.

[6] ie, the way that they structure and organise themselves, interact and 'process'.

- encourage interactions among any and all of its members (eg: loyalty might be not just to local entities, but also to the overall enterprise) and other actors in the environment;
- have 'power' available to be used where it is required (so that users can adjust the extent of their ability to act decisively);
- uncouple command and control from the organizational structure, adding to the 'degrees of freedom' available (enabling them to seamlessly 'morph' organizational structures and flip between states without internal dislocation);
- exploit the phenomena arising from their structures and from the wider environment (which are emergent, defined as arising from the various conditions in place and the myriad of interactions among the environment and other actors).

The perceived advantages of networked organisations are that they are agile and can adapt to any kind of adversary, operational environment, threat or damage - maintaining a persistent identity and purpose over time. In addition they can generate and exploit new means and opportunities - making them difficult to predict or undermine. They are agile, flexible, responsive and robust - lacking single points of failure - making them resilient to shock and dislocation. Their internal plasticity and ability to reconfigure means that they can, potentially, bring all assets to bear on a single crucial issue as easily as they can disperse effort across the world. However, their behaviour will never be completely predictable and, from certain perspectives, they may be inefficient. Finally, because they lack the internal boundaries that weaken power, they can act with unified and coherent purpose (al-Qaeda might be considered to be an extreme example) - even though they, and the loci of actions, are dispersed.

COMPLEXITY AND THE WIDER ENVIRONMENT

The wider environment within which all human activity takes place is a complex adaptive system (CAS), itself composed of myriads of nested complex adaptive systems loosely connected through an ever-changing network of interactions and interdependencies. It is beyond the scope of this paper to discuss complexity in detail, but many good references and summaries exist (see [6, 7, 8, 9, 10, 11, 12]). Overall, this complex wider environment has certain features that we must take into account:

- Complex adaptive systems are ones where the outcomes do not follow in a predictable and repeatable way as they might with a mechanical machine - they generate problems which seem puzzling in their complexity (so-called 'wicked problems' [13]);
- However, they do display various phenomena and behaviours which have identifiable characteristics (eg: stable emergent phenomena arise; networks have useful properties such as their robustness and ability to propagate power, information, influence etc);
- The mechanisms which operate in complex adaptive systems fall into three main types which we can influence directly to our advantage: top-down, bottom-up and self-regulatory / self organising [14]. These mechanisms are always present and they are the ones which can be influenced by commanders / managers of organisations;
- Linkages between purposeful entities and the wider environment are manifested in many types of interdependencies and feedback relationships. It is through these changing linkages that influence is propagated (where complex phenomena shows their hand).

In this paper we intend to show that, despite this, we can both derive pragmatic models of use to the military and business community and, if we employ appropriate strategies and approaches such as those below, can exploit the properties of CAS to decisive advantage in coalition operations and in commerce.

APPROACHES FOR EXPLOITING COMPLEXITY

It is apparent that there are different approaches and techniques which we should be employing when we design, assemble and when we operate enterprises at run-time. To do this, we understand how to exploit the appropriate mechanisms which operate in each of these spaces and should develop them further. Furthermore, we should understand the relationship between the spaces (ie what happens when an organisational unit is moved from, say, assemble-time to run-time in terms of the new opportunities which become available and strategies employed). Networked coalition enterprises are de-facto based on complex adaptive systems and, therefore, during operations, cannot be discontinued at will - they are always connected, always on. This means that, when something needs fixing / changing, we cannot stop, dismantle it, redesign it and try again. Instead, we need a set of on-line techniques available to enable organisational sensing, evaluation, assessment, learning and on-the-fly adaptation of behaviour. We also need to be able to manipulate the run-time environment to shape it to our will. The rest of this section addresses these issues.

THREE PERSPECTIVES - THE DART FRAMEWORK

Given the context described above, strategies are required which recognise the characteristics of networked enterprises and their environments from three perspectives (shown in Figure 1, covering Design, Assemble and Run-Time - the DART Framework). Firstly, enterprises are composed from basic elements whose properties can be characterised at 'design-time'; secondly, these elements are then brought together at 'assemble-time' and thirdly, interactions between the elements and the wider environment only become activated at 'run-time'.

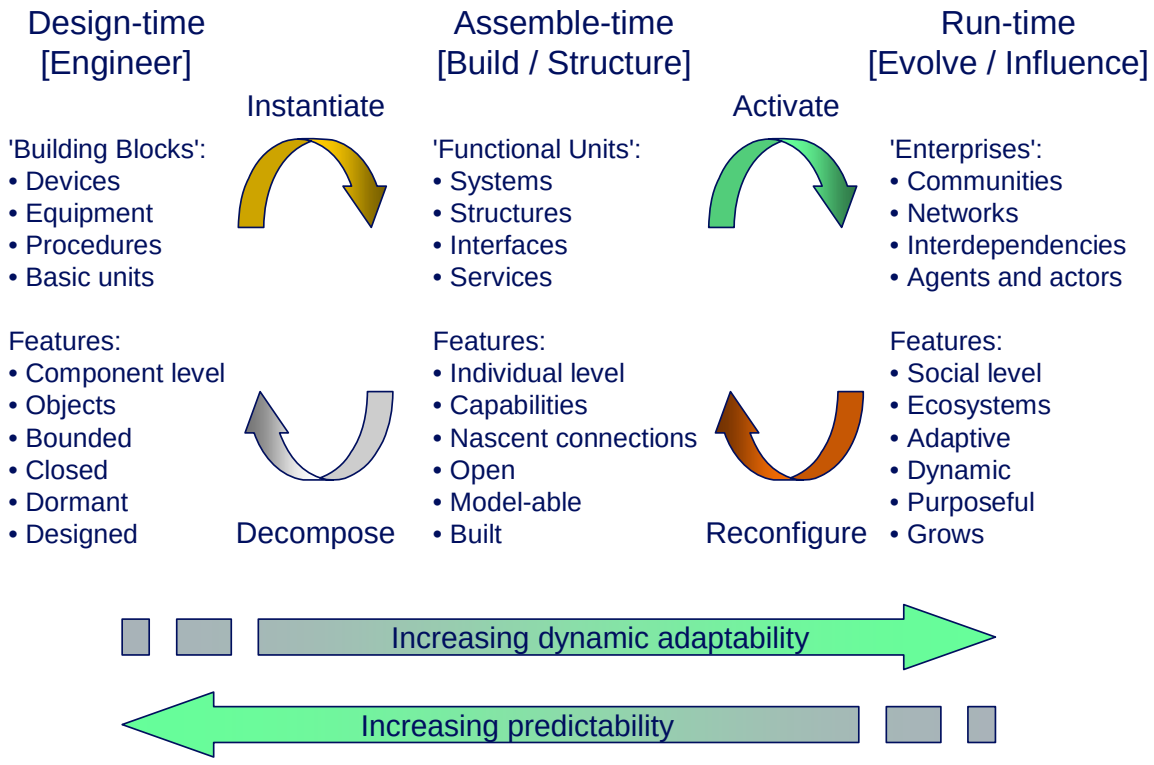

Figure 1 - One view of the DART Framework

If one is to effectively understand and shape complexity to advantage as a 'force multiplier' then the features and factors relating to these three perspectives need further study and elaboration. Key to this is realising that there are limits to what can be achieved at design-time, at assemble-time and at run-time and that these are not separate domains but a set of 'states' that we can flip between as circumstances change[7]. For example, depending on what needs to be done, we can flip part of our enterprise to the appropriate assemble-time configuration, carry out the change and flip it back again, say, into the operational, run-time mode.

DESIGN-TIME

Characteristics of Design-time. Our current approach to dealing with the complexities of the real world often employs system engineering - a design-time methodology. Here, one attempts to identify all the run-time requirements in advance and then develop a solution. In practice, the deployed system is usual constrained to display deterministic behaviour. Worse, existing socio-technical processes are digitised, 'freezing in' outdated or failed ones and limiting the space of options and initiatives which can be seized and exploited in future. Inevitably, the deployment of the system changes the environment and the original premises on which the requirements were based no longer hold - resulting in endless change requests and an inability to either generate novelty or deal with the unpredictability of the real world [15]. Hard won experience [16] has proved that a different approach is needed to generating, deploying and employing structures and systems which can really address complexity. At design-time we determine the basic features of building blocks, define their enduring features (which will enable them to be assembled into more meaningful functional units) and construct them ready for assembly.

Some Mechanisms Available at Design-Time. The key design rule that must be applied is to minimise design-time assumptions in order to maximise assemble-time and run-time flexibility. This is an over-arching rule that includes the principles discussed below.

- Separation and Loose Coupling. Wherever possible, the relationships and interactions of the building blocks should not be fixed at design-time. The ability to interact will be provided, but the range of particular interactions that might take place will not. In computer technology terms, this includes the separation of interfaces from implementation (separating what a element does from how it does it), the removal of hidden dependencies and interconnections (using the interface and nothing but the interface) and avoiding trying to define all information-exchange requirements (IERs) in advance. Loose coupling can be achieved using dynamic discovery rather than using predefined connections and interactions;
- Open Interfaces - Sharing**.** In the human context, sharing and altruism are key enablers for networked enterprises. Here the 'interface' is having the ability and predisposition to converse and exchange information of some sort in a purposeful manner. In technical terms, it is not possible to prescribe how elements will be used in the future, so systems and components must be designed in an open fashion[8] providing interfaces that allow their functionality to be invoked by new, perhaps unanticipated elements. This enables reuse and greatly improves interoperability;
- Separation of Action from Information. In human terms this would relate to the difference between education and mechanistic training. In the former, people can use the information at their disposal in a number of flexible ways. In the latter, only a limited number of behaviours are possible. The more widely available the 'information' the better

[7] We might model aspects of these behaviours with finite state machines - but other techniques are required too such as complexity modelling etc.
[8] For example, compare the fragile performance of an RS232 serial connection with the resilience of USB.

the interaction and the greater the flexibility. In technical terms, generic data formats and ontologies facilitate this, allowing domain knowledge to be expressed in standard flexible ways, and extracting assumptions, processes or doctrine that would otherwise be hard-coded into devices and thus very difficult to change. These approaches use open, enabling standards (as opposed to constraining standardisation) - strongly supported by off-the-shelf tools - such as wrapping heterogeneous data so that it can be manipulated as shared information.

Examples - Exploiting Design-Time Mechanisms. In the context of infrastructure, design-time issues would include, for example, deciding upon the communication bearers and router elements to be deployed and the range of protocols to be supported. It would also include the ability for new protocols to uploaded later. In relation to the provision of toolsets, it could cover the description of the core services to be deployed and identification of a common core set of tools. Design principles would be selected which would allow new tools and services to be assembled in many different ways to support the imperatives of different users and which would allow them to be added on-the-fly at run-time. In organisational terms, at design-time, basic military structures are defined (squadrons, platoons etc) and their Concepts of Operation and Standard Procedures defines. Depending on how this is done, it will can result in rigid, 'brittle' behaviours at run-time or flexible and adaptive organisations. The social aspects of design-time relate to the kind of coalition training that is considered and the social and cultural 'norms' which are written into doctrine or provided (formally or informally) as guidance.

ASSEMBLE-TIME

Characteristics of Assemble-time. At assemble-time we do not build devices - this has already been done at design-time. Instead, for networked coalition enterprises, we are putting together functional units / organisational elements (from whatever building blocks are available) ready to be activated and deployed. At assemble time we carry out the basic reconfiguration such as: changing structural relationships, determining authority, accountability and responsibility and setting initial autonomy, limits, tolerances and degrees of freedom - difficult tasks for coalitions.

Some Mechanisms Available at Assemble-Time. Some of the implications of this are that we should contrive heterogeneous functional units with properties which enable them to be composed / aggregated in various ways - either on demand or spontaneously. Functional units should be provided with the potential to display the following behaviours at run-time:

- a persistent identity over time supported by learning and adaptation;
- the ability to sense, be aware (self and non-self), evaluate, assess and reason;
- the ability to manipulate resources / artefacts and effect change;
- the ability to converse / interact with each other and form persistent relationships;
- the ability to respond to external influence (directed or otherwise).

Therefore, to implement networked enterprises, we will have to harness and intercept the latest developments in these areas to enable decision makers to work in a secure, flexible and agile manner. Without innovative approaches we will have to use our current tools and techniques which cannot cope with complexity and the unexpected / unanticipated and which provide us with notoriously brittle and impoverished solutions. Novel technologies that may be relevant include agile and resilient networking, peer-to-peer computing (P2P), grid computing, Web services, software agents and service-orientated architectures, Semantic Web (knowledge technologies), and human-computer interaction technologies (for more on this topic, see D N Allsopp's paper in the same series entitled "Mechanisms for Agility").

Examples - Exploiting Assemble-Time Mechanisms. In the context of infrastructure, assemble-time issues would include, for example, the basic self-organisation of a network or its configuration according to an initial communications plan. In relation to toolsets, it could cover an initial deployment configuration based on previous best practice or exercises. An explicit assumption will be that this configuration **will** change as soon as it is activated in response to the changing imperatives. In organisational terms, at assemble-time, military units are assembled and start training together. However, some organisations will be assembled ad-hoc (eg: so-called agile mission grouping) and deployed at very short notice - being injected into a fully active run-time environment. For insurgents and terrorists this is a continuous activity, mostly carried on in the run-time environment. The social aspects of assemble-time relate to the formation of coalitions, communities of interest, informal groups and command structures.

RUN-TIME

Characteristics of Run-time. Let us now consider the run-time issues. Obviously, you can't begin to establish the exact performance of components until they interact within the environment and, even then, all that one can establish is an estimate of bounds on behaviour. This is because it is impossible to examine every state under which the components would have to operate as many of the states are emergent and *cannot be part of the formally specified design*. It is the appearance of these emergent phenomena which leads to the failure of many of the attempts to create, for example, national computer systems and is why 'unwanted' emergence is treated as something to eradicate - leading to a retreat away from embracing complexity towards design-time 'certainty'. This paper turns this view on its head and aspires to maximise novelty at run-time. Hence, we have to accept that we cannot rigorously test the 'system' before deployment because, de-facto, the boundaries of the 'system' cannot be defined in state terms. Instead, we will need to provide ourselves with run-time tools through which we can reinforce obligations, adjust authorisations and influence interactions and social behaviour towards our requirements. The run-time tools vary from cultural strategies for influencing behaviour through to software or hardware tools.

Some Mechanisms Available at Run-Time. Networked enterprises will evolve their behaviours and they will become less mechanical and more organic (less engineered and more grown). Part of this comes from having "the ability to reconfigure" available to the organisation based on the interactions which need to occur and the relationships that need to be supported. Implicit in this is the need to be able to recover from dislocation and / or dysfunction. Interestingly, networked organisations will, in many respects, behave as if they are, simultaneously, a single entity and a colony / community / swarm.

When the assembled building blocks are deployed into the run-time environment and interact patterns of phenomena will appear, persist over time and have a manifestation[9] which can be detected and acted upon within some context at a higher level of abstraction. As networked enterprises are based on complex adaptive systems various phenomena will arise spontaneously / be manifested such as: attractors, emergence, reverberatory structures, catastrophe landscapes, co-evolution etc [10, 11]. I would assert that these are essential to the way that networked enterprises will function and, as such, are not optional add-ons.

The key dimensions of agility[10] are all emergent too and include: robustness, resilience, responsiveness, flexibility, innovation and adaptation. In the networked enterprise context, we have the opportunity to detect these new phenomena and use them to generate new effects, but

[9] One example would be the level of morale within part of the force. A dysfunctional example would be a mutiny triggered by some decision on conditions following months of privation.
[10] Agility can only be manifested at run-time - there is no such thing as static, design-time agility!

how do we do this? We have already started on the process by altering the design-time features of our building blocks, initiating structural relationships at assemble-time and by creating run-time tools - these will now take effect as they join the active environment and interact releasing the novelty[11] and flexibility required for networked enterprises. There are three main approaches which can be exploited during run-time: top-down control, peer-level self-regulation or bottom-up emergence.

- Top-Down. There will be 'influencing minds' that will want to manipulate various 'levers' (described further below) and the CAS phenomena to shape and influence the organisation, to: set context and purpose (shared intent); shape organisational structures, force mixtures and allocate power; tune interactions and relationships, degrees of freedom (clamp etc); alter priorities, constraints, authorisations, obligations, incentives etc; foster repair and recovery.
- Self-regulation. However, it would be inappropriate to expect the 'influencing minds' to be continually involved in trying to enforce, say, top-down control. Instead, we should expect networked organisations to be 'autonomic' [17] (self-healing and sustaining by definition) in response to damage, discomfort and opportunities. This is not just about homeostasis[12] in a simple sense. Firstly, it is about having a sense of self and non-self and being aware of form and purpose (and knowing that you have it). It is also about being able to detect change, understand its nature (evaluate) and its significance to the organisation and then being able to assess what it will do to your unfitness (local and global) and then subsequently using this as an imperative for acting / reconfiguring. Repair (shaping and adapting) involves being resilient and in having some notion of robustness and how the effects of the damage might propagate. Quick response may be assisted by invoking (or adapting) 'imprinted' response / react behaviours or by using templates from previous experience.
- Bottom-up. Total control cannot be imposed on complex adaptive systems. Instead, shaping can be achieved and is something which emerges from influencing the behaviours of independent agents. We need to know how to work with the mechanisms of emergence and there are some candidate approaches available which are discussed in [18, 19, 20, 21] and include: tuning interactions; changing the 'population density' (adding or removing different types of units - even destroying them); manipulating the environment (destroying a bridge say); changing relationships (forming new allegiances) and interdependencies (supplier / user dynamics) etc.

Examples - Exploiting Run-Time Mechanisms. In the context of infrastructure, run-time issues would include, for example, dynamic network management and self-regulation. In relation to toolsets, changes will be triggered and accommodated in response to the changing imperatives. This may involve demands for new building blocks, plug-ins or software updates. In organisational terms, at run-time, military units can change their relationships, authorities, obligations and responsibilities if the assemble-time guidance allows it. The social aspects of run-time relate to changes to interdependencies amongst communities of interest, informal groups and command structures. This might relate to the consequences of new coalition partner arriving in theatre or refusing to take part in a particular type of mission. For insurgents and terrorists, this may involve changes in short-term alliances between warlords or agreements to work together for mutual gain (franchising).

[11] Which may be social, co-evolutionary or may involve manipulating the environment directly or indirectly etc (ant ants do as a way of signalling between each other - so-called stigmergy). There are a rich set of influences available which have been discussed elsewhere [14] and which are rarely employed.
[12] The apparent stability of an ecology / organisation / organism (such as in the human body) which arises from the interactions between the various dynamic activities of self-regulation.

SUMMARY

This paper has noted that throughout the worlds of military enterprise, commerce and government and in everyday life we are increasingly connected through complex networks of relationships and interactions which may be considered at different levels of abstraction. For organisations, the key word is agility - being able to adapt to and shape the uncertainties of the world without dislocation, which is as applicable in the cyberspace that supports them as it is to the real world that they inhabit. For true agility, networked enterprises and cyberspace must, in concert, be capable of supporting a continuous process of dynamic, innovative change where many effects and behaviours will be manifested as emergent phenomena. This paper has considered some of the mechanisms which can be exploited at design-time, assemble-time and run-time to enable this - influencing the structures and relationships in networked enterprises and ensuring the collective, adaptive and secure behaviour of entities in cyberspace. The focus of this paper has been on how to leverage the complexities of the real world, at run-time, to achieve decisive advantage for coalitions. The key points were that:

- The world is complex - we can't avoid facing up to this as the military business becomes more fluid and networked into everyday life where threats come right to our doorstep;
- Many current tools and techniques cannot cope with complexity and the unexpected / unanticipated and provide us with notoriously brittle and impoverished solutions;
- The wider environment, complex adaptive systems and purposeful organisations built on them can be characterised in a manner which provides us with a straightforward language for reasoning about the challenges and opportunities;
- Suitable design, assemble and run-time (DART) mechanisms and approaches exist for turning complexity to advantage and the paper offers them, and the methodology for deciding when it is appropriate to use them, to the community for discussion.

REFERENCES:

[1] Patrick Beautement, David Allsopp, Mark Greaves, Steve Goldsmith, Shannon Spires, Simon Thompson, Helge Janicke. "Autonomous Agents and Multi-agent Systems (AAMAS) for the Military - Issues and Challenges" published in "Lecture Notes in Computer Science". From: http://dx.doi.org/10.1007/11683704_1. Defence Applications of Multi-Agent Systems: International Workshop, DAMAS 2005, Utrecht, The Netherlands, July 25, 2005, Revised and Invited Papers Editors: Simon G. Thompson, Robert Ghanea-Hercock, 2006. Publisher: Springer Berlin / Heidelberg

[2] M Kirton et al. *The coalition Agents Experiment: Network-enabled coalition Operations*. In Journal of Defence Science (Special edition on NEC), Vol 8, No 3, Sep 2003.

[3] Coalition Agents Experiment Web site: http://www.aiai.ed.ac.uk/project/coax.

[4] Bradshaw et al. *Making Agents Acceptable to People*. In Intelligent Technologies for Information Analysis. N. Zhong and J. Liu (Eds.). Springer 2004.

[5] Comments by MC Meigs, former Commander of SFOR in Europe, see http://carlisle-www.army.mil/usawc/Parameters/03summer/meigs.htm

[6] See extensive research material on complexity and related topics on the Santa Fe Institute site: http://www.santafe.edu/sfi/research/focus/networkDynamics/index.html

[7] Complexity Science - Network of Excellence: http://www.complexityscience.org/

[8] John H Holland. *Emergence: from Chaos to Order*. p7 Oxford University Press. ISBN 0-19-286211-1. 1998.

[9] Steven Johnson. *Emergence. The Connected Lives of Ants, Brains, Cities*. Penguin.

[10] Morowitz, Harold J. *The Emergence of Everything : How the World became Complex*. Oxford University Press, 2002

[11] Patrick Beautement. *Exploiting the Phenomenon of Emergence as a Force Multiplier*, at http://www.tbt.org.uk/

[12] Roger Lewin. *Complexity - Life at the Edge of Chaos*, Phoenix 1993.

[13] Tom Ritchey. *Wicked Problems - Structuring Social Messes with Morphological Analysis*. Swedish Morphological Society 2005. http://www.swemorph.com

[14] Patrick Beautement. *Controlling Edge Organizations: Exploiting Emergence*. Paper 115 at ICCRTS June 2005.

[15] Guy Kirsch in Chap 1, *Artificial Life and Virtual Reality*. Wiley 1994.

[16] Colonel John D. Rosenberger. *The Inherent Vulnerabilities of Technology: Insights from the National Training Center's Opposing Force*. U.S. Army, 2002.

[17] See http://www.research.ibm.com/autonomic/ .

[18] Jennings, N R. *An Agent-based Approach for Building Complex Software Systems*. 2001. Communications of the ACM, 44:4, 35-41.

[19] Stephen Wolfram. *Cellular Automata as Models of Complexity*. Physica 10D. 1984.

[20] Eric Bonabeau, Marco Dorigo, Guy Theraulaz. *Swarm Intelligence: From Natural to Artificial Systems*. Santa Fe Institute Studies on the Sciences of Complexity.

[21] Beckers, R., 0. E. Holland, and J.-L. Deneubourg. *From Local Actions to Global Tasks: Stigmergy and Collective Robotics*. In *Artificial Life IV,* edited by R. Brooks and P. Maes, 181-189. Cambridge, MA: MIT Press, 1994

P Beautement
Malvern, April 2006.