Challenges for Joint Battlespace Digitization (JBD)

S. Hamid, I. White and C. Gibson
Defence Evaluation and Research Agency (DERA)
Portsdown, Fareham, PO17 5EU, ENGLAND
shamid/iwhite/cgibson@dera.gov.uk

Abstract

This paper highlights several important areas in achieving extensive integration of military command and control systems. The discussion in the paper focuses on two areas where technology per se is deficient, and that must be considered carefully against the stronger tides of technology push in systems design and acquisition. These areas are the human factors aspects of system design, and the challenge of information management

1. INTRODUCTION

1.1 Background

Several of the NATO countries have proposed more integrated defence IT infrastructures to help achieve information superiority. It is, of course, a truism that information superiority will give a party an advantage in any conflict, and historic examples abound, perhaps the most famous from a British perspective being the use of the Enigma decodes during WW2 [1].

It is the nature of defence acquisition that the information systems inventory will comprise a range of systems of different capabilities and technology vintages. At the present time, the UK inventory includes old bespoke military systems coupled with modern IT systems having a high commercial off-the-shelf (COTS) element. Information superiority requires, amongst other things, that this mix of systems be integrated into an interoperable, 'seamless' whole.

This vision of seamless Defence IT has spawned several national initiatives that seek to help achieve it. In the UK this is embodied in the Joint Battlespace Digitization (JBD) initiative that seeks to provide a wide range of interoperability benefits that will take UK defence well towards the information superiority goal.

The goal of information superiority requires a whole range of technical and non-technical changes in all aspects of defence capability - doctrine, command processes, organisations, user-requirements specification, architecture definition, technology development and exploitation, procurement, training and operational use.

In this paper some of the challenges are examined and the prospects for progress reviewed. The emphasis is on the definition of systems and their implementation in modern technologies. This encompasses the definition of a systems concept, an integration architecture, and the ability to realise many of its elements using COTS services, systems and elements. By integration architecture is meant a collection of rules, recommendations, process definitions and standards that apply across all systems.

The paper highlights in particular the issues of human factors (HF) and information management (IM). These have been chosen here because there are still many unknown and therefore significant risks in these areas.

1.2 Major Technical Issues for JBD

At the technical level many major problems have been identified that need to be resolved through defence-sponsored research. Others are better left to the commercial world to resolve. The decision about which issue is in which category is itself a critical technical risk! A shortlist of the issues being addressed within the UK defence research programme are grouped under the following headings:

- Future command concepts and business processes
- Human Factors
- Information management
- Information technology and systems
- Systems Integration

Paper presented at the RTO IST Symposium on "New Information Processing Techniques for Military Systems", held in Istanbul, Turkey, 9-11 October 2000, and published in RTO MP-049.

In this short paper it is impossible to describe all the solutions being pursued within the UK to meet these issues. This paper therefore gives more attention to human factors and to information management than the other topics. There is a degree of euphoria surrounding new capabilities in information and communications technologies (ICT) and the related, the exploitation of COTS developments. It can be easily forgotten that command information Systems (CIS) are to meet human needs, and that the system design aspects that focus on this are still very poorly understood, and inadequately applied. First the key issues concerned with user needs are outlined.

2. USER NEEDS

2.1 Comment

It is a half-truism that the in-theatre user lacks the vision to see the technological possibilities of the future, and the visionary lacks the experience of real users to provide what is really needed. This belies the real situation whereby with careful liaison between these groups a reasonable prediction of needs can be attempted. For success, users' aspirations and technological possibilities need to be aligned, but the chain of dependencies is not well understood. The issues are understanding:

- distributed operations
- the needs for 'synchronysity' (making the right actions occur at the right place and the right time over a very distributed network of decision makers and organisations)
- satisfying manourvist warfare principles.

Current design techniques are based on workshop methods (story boarding and ad hoc diagrammatic representations, that often retain a strong degree of ambiguity). What technologies exist to help us here? There are a range of soft-system methodologies prescribed for the better definition and elucidation of such issues [2], [3], [4]. DERA has invested substantially in high level information flow models to represent the information exchange behaviours of emergent new social structures of command that are consequences of the changes in both technology and in warfare concepts. This work however would need another paper to describe it.

3. HUMAN FACTORS

3.1 Cognitive Dominance

Central to the achievement of information superiority and military objectives is the very human concept of *Cognitive Dominance* [5] – going beyond information dominance to have the ability to exploit this superiority. This concept has the following six aspects:

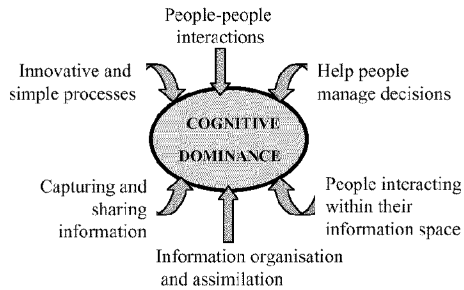

Figure 1 – The six aspects of the concept of Cognitive Dominance

ICT (i.e. digitization) is a key enabler of cognitive dominance, but in realising it a balanced organisational change process is needed. As Figure 2 shows, technology is but one of four forces of change that the Joint Battlespace Digitization (JBD) initiative aims to bring into dynamic stability [6].

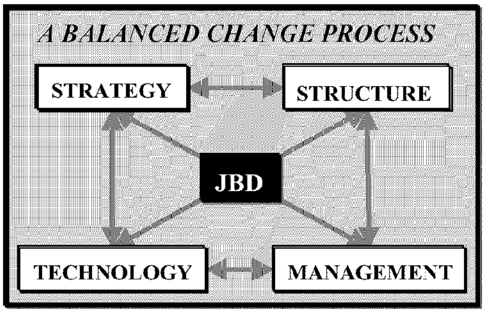

Figure 2 – The four forces the JBD change process needs to balance

Important human factors issues permeate all four forces. These are discussed below according to the schema in Figure 2; Figure 3 indicates the scope of each of theses forces, as discussed below and shows how they inter-relate.

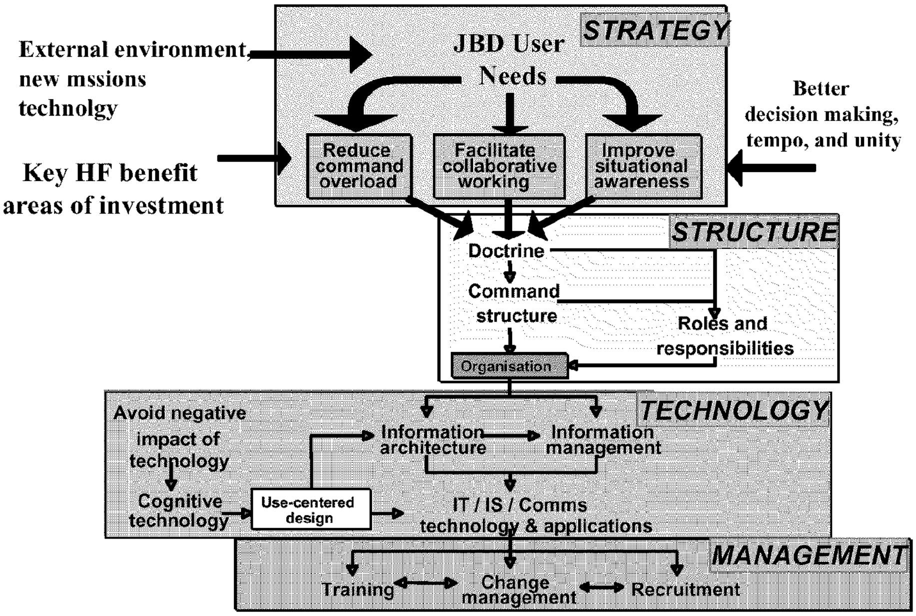

Figure 3 – JBD - A view of the inter-relationships between the four forces

3.2 Strategy

In essence the aim of JBD is to enhance perception and situational awareness (i.e. lift 'fog') and increase action options (reduce 'friction'), thus allowing command to cycle more quickly (i.e. better decisions and tempo). This leads to the desired force agility and flexibility. If however, as is highly likely, 'fog' and 'friction' are still key problems of future military command, we should expect the emphasis to shift to the qualities of the commander, in particular to his cognitive abilities. Such commanders must be able to synthesise information from a great variety and number of sources (e.g. political and military), particularly in complex diplomatic-military operations in a multi-national context, to achieve a true sense of what is going on.

Related to the above JBD aim from a human factors perspective, the three key benefit areas of investment in JBD are that it should [7]:

- reduce command overload,
- facilitate collaborative working, *and*
- improve situational awareness.

These are part of the JBD User Needs at the level of strategy (see Figure 3). In combination these three benefits contribute to the achievement of all six aspects of cognitive dominance, that should lead to better decision making and operational tempo, and unity of effort. Some of the command level problems induced by technology are outline later.

Reduce command overload: This is best achieved by reducing the amount of cognitive processing required and the number of activities an individual has to attend to. Measures include presenting information in an integrated fashion, simplifying processes (e.g. reducing the number of manual steps), and having standard operating procedures and doctrine for dealing with a situation or issue. Often we cannot tell in advance what information may prove to be highly pertinent, so that staff and commanders must operate in surveillance mode, scanning and sifting for useful items. To some extent this dilemma can be addressed through collaboration among commanders and staff or through organisational procedures and systems. Intelligent systems that are able to highlight changes and key factors will also help here.

Facilitate collaborative working: Joint and Multinational operations demand effective teamwork towards shared military objectives. The key issue here is providing support to those activities related to communication, co-ordination and the development of shared understanding within a team, including both distributed and ad hoc teams. Technological support for such teams is currently immature. Recent improvements of the understanding of team processes and teamwork challenges encountered by military personnel operating in distributed and ad hoc teams can be used to highlight technological design imperatives for computer-supported collaborative working.

Forms of data fusion support are required that are more in tune with the socio-cognitive processes by which humans collectively integrate information, and the fundamentals of military practice.

Improve situational awareness: This has three components of equal importance: the ability to understand how a situation has developed; the ability to comprehend the current situation; and the ability to predict how the situation might develop. What is important is having the right information and cues at the right time. From an information presentation perspective, use of tactical picture agents for monitoring and alerting as part of the strategy for the management of operator attention can help.

3.3 Structure

The new missions in the changing operational environment, together with digitization technology make ad hoc 'teams' more attractive as a way to get jobs done – the challenge is to facilitate effective teamwork in such ad hoc situations. Flatter command structures to maximise agility and force flexibility enabled by the information age and are seen as inevitable. Driven by these pressures, it is not surprising that the armed forces should consider more loosely-based federations of functions to perform a mission in a self-synchronous way; noting that organisational and team loyalty are still important to the bonding process and team resilience. Future CIS structures may therefore be loose aggregations of autonomous units rather than rigid hierarchies, since the CIS organisation requirement depends on the ratio between CIS speed and battle speed. As noted in [8] "the more fluid the circumstances, the lower the decision level should be set"

Digitization allows integration of organisational functions at all levels, both within and between organisations. In order to achieve this, management must effect changes in organisational strategy, structure, processes and culture (possibly only at the artefact and attitude level rather than at a deeper social level). Information and communications technologies (ICTs) have implications for the boundaries of the organisation, and the ability of managers to control the flow of information. If information is power, people are likely to be reluctant to give it away. Management must therefore create the environment in which people will share information. The speed and extent to which organisations may move in this direction is constrained by their current structures, process, skills and expertise, and their investment in existing (legacy) information systems. However, the greatest inhibitor may be the legacy organisational culture and practices.

Organisational structures are affected by the changes in the way work is done as a result of ICT developments – for example, new specialists, fewer unskilled and semi-skilled employees. There is a need to define and delineate the new roles and responsibilities within a digitized organisation, taking into account recruitment and retention problems. Clearly, organisational re-structuring should be aligned with doctrine, and tools, techniques and procedures. A use-centred philosophy should be employed where the emphasis is on simplifying the processes, and using technology to support skilled staff to enhance their productivity [9].

3.4 Technology Implications from HF

JBD architecture from an HF perspective: The JBD information architecture encompasses a cognitive dimension as an overarching top layer. This is because at the cognitive level individual and group perceptions provide understanding and they influence decisions and people. Furthermore, meaning is often extracted by the humans from information outside of, and ahead of, the supporting information system. Information management is therefore not merely a question of computer systems and information and communication technologies. The following four inherent limitations and shortcomings of computer-based information systems further illustrate this point [10]:

- There is a large amount of key information and knowledge that is not captured by or represented in these computer-based information systems.
- Important but unpredictable or anomalous organisational processes are unlikely to be supported by a computer-based information system.

- Current ICT systems only present to the decision-maker that information that has been identified as being of value by the designers and procurers of the system. They are unlikely to have thought of every eventuality and circumstance.
- Information gathered by current ICT systems is historical - they have little predictive capability.

The focus of information management should be on management processes and organisational implications. The emphasis of technology considerations should therefore be on the use to which technology is put in organisations. A use-centred information management considers the ways that managers and staff *actually* use information to drive the development of computer-based information systems, rather than imposing some idealised or normative technical solution on the people in the organisation [10].

Communications systems design must remember that communications between people is naturally a human process, where:

- The message itself is not necessarily unproblematic – the sender may be struggling to express it precisely.
- The context is very important as other messages may be competing for attention.
- The expectations or perceptions of the recipient can generate particular interpretations.
- Likewise, the medium used to convey a message can affect perceptions.
- Non-verbal elements are very important in human communications.

Organisations cannot function without managing their information processes effectively. Within the organisation, knowledge is within the heads of the workforce, is embedded in tools and machines, as well as being captured and represented in organisational processes and heuristics.

The ability to learn is crucial, so that information processes have to be dynamic. Information processing requirements should be derived from CIS requirements on critical information needs, team interaction requirements, display and software design imperatives, physical configuration of command post, decision support tools etc.

Automation of task and data management has a strong impact on human behaviour and task requirements. Automation often gives rise to new tasks (such as management of information) and responsibilities (such as data ownership, access and control of data). Adaptation behaviours also give rise to systems being used differently from that anticipated.

There is still a huge amount to understand about the relative overall costs of handling information in different ways, and the ease or difficulty of ensuring up-to-date and accurate information under different arrangements. These questions are inextricably bound up with the crucial people issues of motivation, job design and staff development.

Command problems exacerbated by technology: There are three potential command problems that may be made worse by inadequate future CIS [11]:

Cognitive overload: Future digitized combat threatens to stretch commanders' cognitive resources much more than before, while still being just as stressful physically and emotionally. Cognition capacity can be enhanced through appropriate method of presentation of information and by the experience and training of the individual who is trying to encode the information. Future CIS interfaces should present information in an appropriately aggregated and individually configurable manner to commanders. A further risk is 'information pursuit' – the more readily assimilable information that is provided the more the commander may pursue additional information, often to the detriment of the operation.

Over-controlling command style: In collective training, due to increased availability of information through digitization, unit commanders have repeatedly been observed using an over-controlling command style. As a consequence junior commanders' initiative is stifled and the decision cycle is slowed due to unnecessary upward referral of low-level decisions. If from the senior commander's perspective 'perfect control' is possible, it may lead to micro-management that overall will have a negative effect on performance.

Big-picture blindness: Not only does this mean that a commander focused on detail will be more likely to miss the big picture, it may also mean that his method of coming to a decision is altered by digitization. Although under normal circumstances the brain manages to integrate the parallel functions of its two hemispheres (on detailed and global processing) to produce coherent behaviour, systems could be designed and used to reduce the risk of big-picture blindness.

Technology pitfalls summary: Many attempts to support the command process with technology fail because the design of the latter is founded upon an inappropriate decision-making paradigm [12]. The design of decision support systems should be based upon an understanding of how people actually make decisions in the real uncertain world, and also upon what they need to do to make these decisions. There is a need to ensure that systems provide information in a manner that is cognitively compatible with the user's mental model and decision strategies. Common problems with inappropriate technological support for command have been found to be:

- User frustration at feeling tethered to workstations.
- Digital mapping used in parallel with the paper systems they are supposed to replace.
- Automated position plotting on digital maps reducing user engagement and thus situational awareness.
- Teams having difficulty in brainstorming around a digital support system.
- Teams having difficulty in using digital maps for situation and mission briefings.
- Lack of system transparency, i.e. lack of understanding of where digital information comes from, how it has been integrated and how it has changed over time. This can thus reduce understanding about how the situation has evolved, and lead to surprise.
- Individuals spend their time 'driving' systems, including information pursuit, that significantly reduces the time available for thinking and talking about problems they are dealing with.

Systems that are difficult to use will not be used widely, particularly under combat stress. This leads to longer terms problems of complacency, skills decay and job dis-satisfaction.

3.5 Exploitation of cognitive science and technology

Recent advances in understanding of the mechanisms of cognition offer opportunities for developing more effective military processes and systems. A satisfactory model of how humans separate and integrate information can be used in the design and development of all systems in which the operator applies cognitive effort. Through an understanding of how sequences of events are separated and integrated by the brain into a 'cognitive stream', guidelines for the presentation of multi-modal sources of information can be formulated.

Cognitive design for human-computer interface (HCI) is concerned with the presentation of information in a manner that converts potential cognitive tasks into perceptual tasks. This is a critical issue underling the design of HCI for use in situations of high workload. Visual and perceptual tasks can require little or no apparent cognitive effort. Thus for an HCI that is used frequently, in a time pressured situation, a simple saving in one element of a display may reduce significantly the user's overall cognitive burden. This leaves more effort available for dealing with (i.e. thinking about) uncertainty and risk in decision making.

Beyond information presentation is the possibility of using real-time adaptive automation and adaptive decision aiding [13]. These use *inter alia* cognitive control theory to consider the effects of time pressure and uncertainty on decision making. The aim is to enable the decision-maker to concentrate cognitive capabilities on the important aspects (i.e. dealing with uncertainty) whilst off-loading routine activities to automation (i.e. alleviating time pressure). This allows the decision-maker to remain in a feed-forward loop whilst feedback can be automated using decision aiding. The main features of such a tasking interface are:

- a shared mental model between man and machine;
- the ability to track goals, plans and tasks; and
- the ability to communicate intent.

Use-centred design as the way ahead: Two fundamental observations can been made concerning the development of technological support systems to-date [8]:

- Much of the technology that has been, and is being developed, for supporting joint and strategic command comes from a technology 'push'. Consequently, the organisation often ends up being 'fitted' around the technology rather than the organisation establishing and defining its technology requirements.
- The design process for the production of technological support systems rarely takes proper account of the critical human factors identified in this paper.

The solution to these two problems is easily summarised, but more difficult to provide in prescriptive form:

- Develop the support technology from a holistic perspective. In other words, understand the nature, values and goals of the whole organisation; the key tasks that it undertakes; the relationship between technological and human function allocation. This can be used as a basis for driving technological development.
- Adopt design approaches that are 'use-centred'. If appropriate, use specialised methods to understand the nature of all the tasks that the humans undertake (including cognitive tasks) and provide this understanding as an input into the more traditional constructs managed by other systems analysis methods. For success, it is imperative to exploit the synergies arising from the convergence of information science, business science and cognitive psychology in the context of JBD.

Empirical studies are essential to validate conclusions on technology design and use, e.g. on organisational and physical design of HQs. Such designs should be based on meeting the requirements of the command function, e.g. physical layout, allocation of function including adaptive automation, distributed and ad hoc team working etc.

3.6 Management

In parallel with the developments in strategy, structure and technology, there is a need to develop cultural acceptance and user confidence. This is concerned with the way individuals, teams and organisations adapt to system changes. Some effects will be cognitive, such as skills fade with the need for amelioration (e.g. through training), whilst other effects will be emotional, such as change in the levels of trust and system dependency.

There will be a requirement for changes in skills and knowledge across the entire armed forces. This will be in part due to the use of new technology, and in part due to the need to conduct command decision making in new ways (including liaison with political, non-government, and other nations' groups). In addition to these higher level changes, indirect skill requirement may take the form of critical thinking and meta-cognition skills, reversionary mode skills, and alternative staff management skills. One of the most commonly cited reasons underlying failures of technology when introduced into military organisations is inadequate training, which results in delayed or reduced uptake and exploitation of technology.

There seems to be an assumption that we will need to recruit and retain more IT specialists as systems managers of the new digitized command, control, communications, and information systems. However, there are doubts that sufficient numbers of people will be available, and, if available, whether they will be easy to retain. Fortunately, there is an alternative approach: as a matter of design principle, make the systems so simple to use and maintain, or support them with intelligent aiding systems, that the need for true IT specialists is correspondingly small. This has two advantages: first, the requirement for specialists would be more likely to be tailored to the very small potential supply; second, the systems would be more usable by individuals and groups who are short of sleep, hungry, thirsty, frightened, and angry – in short, who are experiencing combat stress.

Finally, a major challenge for management will be to lead their organisations through the transformation necessary to prosper in the globally competitive environment. When the issue at hand is organisational transformation, enabled by technology, it appears particularly important to invest sufficient time and effort in getting the organisation to understand where it is going and why. The people issues are critical in the transformation process. One root cause for the reported lack of impact of ICT on the improved performance of commercial organisations is an organisation's unwillingness to invest heavily and early enough in human resources. The armed forces must therefore learn this lesson and invest in new skills, in psychological ownership of the change process, and in a safety net under the employee so that there is no fear of taking prudent risks. These investments are required throughout the defence organisation as management itself is part of the required change.

4. INFORMATION MANAGEMENT

4.1 IM Definition

The need to meet the HF aspects in new systems design and operation has its counterpart in the definition of, and management of, information. With the creation of distributed operational staffs, powerful communications and powerful IT have highlighted our poor ability to manage the vast amounts of information to which we have access,. Much of this information is stored in a variety of formats, and with little consistency in terms of structure of storage, time stamping, formatting. presentation, precision and communications form.

The definition of IM is a source of argument, but the following covers the scope addressed by this paper:

Information Management is the control (creation, direction, filtering, presentation and deletion) of information between users in all defined domains at all communications, middleware and semantic levels (as defined below).

To be fully effective it is easily shown that management at each of these three levels is needed, and that there must be strong management interactions between these levels.

4.2 The IM Problem

The IM problem is simply that the wide variety of national CIS systems (land, sea, air, joint and coalition), in a JBD environment must inter-operate to varying degrees. Not only are these CIS constructed to represent data in ways matched to the specific 'sub-culture' of their users, the technical solutions are also widely different. Database schemas and their update and configuration control regimes and HCI vary. Furthermore the systems cover a range of procurement periods, ranging from full legacy to modern systems using a wider range of concepts and technologies to provide information to CIS users. IM is essential to manage and distribute such diversity of information to those who need it in an integrated, timely and expedient way, taking full account of the HCI issues outlined in section 3.

4.3 An IM Model

An IM model for examining information management is:

- a society of agents, who have some degree of common culture (agents may be men or machines)
- a repository of information (static and dynamic, created, deleted, growing and decaying)
- a set of goals (also static and dynamic).

The achievement of these goals is facilitated by information agents having the right information at the right time in the right place, and in the right form. This is of course an ideal posing many difficult questions. IM needs to act at three levels:

1. Semantic
   - Context correlations
   - Domains (whose members collectively invent sub-languages)
2. Applications
3. Communications/networking

This is shown in Figure 4. The diagram is explained from lower to the upper levels.

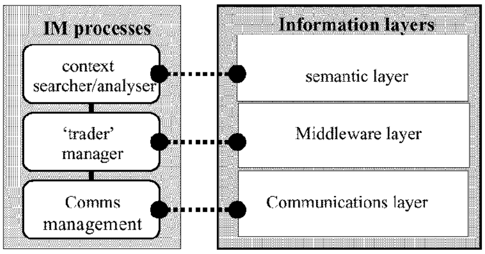

Figure 4 Layered model of IM

Communications layer management (CLM) can monitor who is communicating with whom, and at what rates, can note fault conditions, and can detect unusual traffic patterns, security violations etc., and control the parameters of the communications network. Communications management must interact with middleware management.

Middleware layer management (MLM) can monitor and control applications interactions, who is using what applications, with whom, what types of file are being interchanged. It can assign and administer priorities, and control other middleware functions such as data caching. MLM can effectively implement load-balancing between information and communications levels, referred to here as 'trading'. MLM can also detect anomalous behaviours.

Semantic layer management (SLM) is the control and monitoring of all the information interactions (deriving from the meaning and intentionality) of the society of agents who seek to meet that society's goals. The SLM must interact with the MLM. This level of information management is concerned fundamentally with the range of human factors issues described in section 3.

Management at each of these different levels contributes to the management of information. Some are better understood than others. The integration of the layer interchanges, and other more sophisticated interactions have not been extensively studied.

4.4 The Problem with IM Models

The problem with this IM, and similar schemes, is that the development of IM into a fully inter-working schema is seen as a long-term task, requiring the solution of some hard problems. Some of the tools from the COTS world are of benefit in implementing IM, notably agent technologies, object schema such as CORBA and advanced mark-up languages such as XML. The work needed to develop and embed such schemes across a wide and diverse range of CIS is nonetheless a major undertaking.

In the following sections the three layers are described further, working form the lowest layer to the highest. This is in order of increasing difficulty

4.5 Communications Layer

Instance of Communications: It is fundamental that a society of agents can only be a society by the cohesive process of communication. The International Organisation for Standards' (ISO) open systems interconnection (OSI) 7-layer reference model, defines all communications around the concept of an *instance of communication.* Each *instance of communication* is described by a set of basic features [14]:

- Sender (identified by an address)
- Receiver (identified by an address)
- Communications set up
- Transfer of data
- Communications clear down
- Duplex/half duplex/simplex
- Duration
- Quality of Service (QoS).

The model also represents the communications process in a layered sense, with the higher layers being more abstract, the lower ones more physical. The ISO model of agent interaction (i.e. the instance of communication) is a fundamental element for a society of interacting agents.

Communications Management: In a given network the various data flows between users compete for the available communications resource[1]. When communications resources are not available, specific communications may be delayed or destroyed. Communications protocols have in-built protective mechanisms to control congestion, most of which involve the loss of information. The criteria for optimising the flows of information are based on various definitions of data exchanges, e.g.:

- Continuous bit rate [hard real time][2]
- Variable bit rate
- Available bit rate.

Protocols exist for establishing reserved paths through networks, but these are not usually an efficient means of using communications resource. The key routes to managing communications resources include:

- Circuit switching
- Packetisation
- Dynamic routing
- Store & forward
- Data shedding (throwing data away)
- Priority and Pre-emption (P&P) mechanisms.

Priority and Pre-emption: P&P requires the user to determine the priority of a message (i.e. instance of communication), and the network to then adjust the bandwidth and the queuing order according to rules based on these priorities. There are many incipient problems with such priority schemes including:

[1] Bandwidth, switching capacity, QoS provision, notably time critical delivery, and error characteristics.

[2] Definitions have been developed by ISO for Time Critical Applications (TCA's)

- What is the QoS of each prioritised communication?
- How large is each communication (how does this impact on its allowable priority)?

Commercial products and protocols exist for most of these processes, and all aspects are subject to continuing development.

The issues raised by implementing P&P in networks has important implications on the middleware layer. P&P is of particular interest for military networks because the concept is long standing, has been implemented in some military communications networks, and is still a requirement. This is discussed further in the Middleware Layer section, 4.6.

Network management status: Network Management (NM) concepts and technology are relatively well developed, and are generally effective, provided the overall mission needs are well understood and mapped into a sound network management strategy. Standards and related protocols are available from ISO, ITU, and IETF, the Telecommunications management forum (MTForum) and there are many useful products UK work is concentrating on developing a concept of operations for network management. The civil concept of NM is focused on service delivery, service growth, and revenue and market capture. Accordingly the development of public domain process models (e.g. within the TMF) is focused on these objectives. The military users must accept that these are not their objectives, and accordingly these need different process models. The implication is that the military must develop the required models themselves.

Interoperation with the MLM; *Inter-operation requires that values of priority labels, and of QoS, are available from the middleware layer, and that status messages from the network are communicated to the middleware layer. More sophisticated interchanges may also be needed, as discussed further in below.*

4.6 Middleware

Middleware Layer – scope: The term middleware is used here to indicate processes above the level of communications, and below the level of information comprehension and use (i.e. the semantic layer); see Figure 4. Many of the middleware operations and concepts assume information need is defined somewhere, but does not itself need to 'know' what that information definition is. Thus:

- QoS must be defined
- Priority labels need to be defined in terms of some functional range (e.g. routine/urgent/flash)
- Data flows over the whole network can be minimised by using file caching strategies, related to information exchange needs. These strategies must be formulated.
- The models of information exchange are logically similar to the connection oriented communications definitions, that are based on the concept of *an instance of communication*.

All of these ideas are discussed here under the heading of 'middleware'. It is accepted that some readers may feel a particular middleware topic is really a communications, or semantic layer issue.

Quality of Service (QoS): The various parameters defining QoS must be related to the users' needs. These can be defined in semantic terms, then middleware terms and finally in communications QoS terms, in a way that is technically meaningful to communications systems designers and service providers. An issue that has received little attention is the extent to which users are prepared to negotiate QoS when the communications or middleware layers cannot provide the QoS requested.

Assigning Priority labels: Across a community of users each 'instance of communication' needs to have some *priority label* attached to it. The rules for attaching such labels will depend upon organisational factors such as:

- Seniority of the person using the priority label
- Significance of the role of the agent undertaking some task.

Note that these are cultural parameters of the society of agents (e.g. what context determines a *Flash* priority, and what service does the user expect *Flash* to imply?). Assigning priorities must itself be a process that is also assigned, i.e. individuals will be given the right to assign priorities. These rights may, from time to time, be changed, revoked, issued etc. and be further subject to restrictions based on any of subject, file-type, file-size, and classification.

The assignment of priorities does not necessarily result in a more equitable data flow through a communications network. It is generally true that provided only a small proportion of the total data within a network is allowed high level P&P labels, an overall gain is made in communications efficiency.

It is fundamental that a good P&P scheme, in which priorities are assigned at the user middleware level, includes interaction with both the communications network, to establish a balance between what can be communicated, and the semantic level, to accommodate what the set of all users wish to communicate.

Data flow monitoring and caching: By observing data flow, not just at the level of bits or packets, but in terms of higher level entities such as files, or logical documents, substantial savings in data flow can be achieved by data caching. The classic example is web browsing, where local servers can hold frequently called pages and save significantly on the demands on the wide-area communications. With such schemes servers need only be sent updates of such pages.

Balancing Mechanisms at the Middleware/Communications Layer Boundary: These are needed when there is some mismatch between agents needs, normally achieved by some feedback mechanism. In the case of the middleware/communications layer boundary, data sources need information on network loading/congestion. For example P&P is in effect assigning a crude value-measure to messages, by setting a high value on the delivery of high priority messages. It is clear that for a JBD society, rich in information, a simple priority system is not sufficient, because it does not guarantee delivery QoS, nor do all message interchanges have similar QoS needs, e.g.:

- What defines satisfactory delivery? (milliseconds, seconds 10's minutes, 1 hour etc.)
- What is the influence of message size? (short ADAP-P3 message; digital image etc.).

These differing criteria must have effects on the overall P&P process and they need to be taken into account in any IM schema.

Middleware schemes for prioritisation can allow each independent server to provide arbitration between users' needs and communications capability, for all users wishing to send information to other users. What these schemes do not usually have (in any depth) is interaction with the communications network (or its management system) nor with other servers on the network. Commercial bandwidth managers for IP (internet protocol) networks do include, in some cases, the ability for different bandwidth managers to communicate, and perform some degree of overall network load balancing.

Given that the various QoS schemes, prioritisation labelling schemes and the information exchange requirements (IERs) and network topology and capacity are defined, information management, at the levels of communications and middleware, can be established by analysis and optimisation modelling.

4.7 Semantic/Middleware Layer Boundary

Instance of information exchange: Just as communications can be described in terms of an instance of communications, so we can also extend the concept to an instance of information exchange. This requires a minimum of two intelligent agents, a common context for information exchange, a process for exchange and a communications channel. The idea is illustrated in Figure 5.

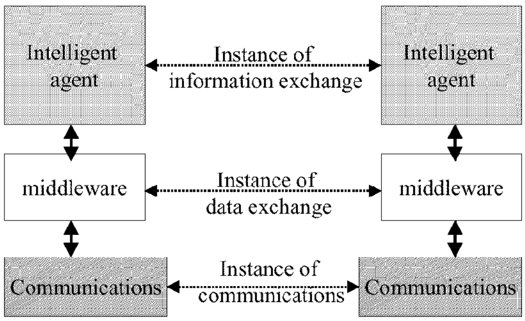

Figure 5 'Instance of Exchange' model

There are various social and motivational models of information exchange:

- Pull (I need to know about *X*)
- Push (I deem it appropriate for you to be informed of *Y*)
  - Agent to agent/agent to object
  - Agent to many (list or broadcast)
  - Acknowledged/non acknowledged.

The implications of information exchange are varied and may be merely informative; more generally information exchange is a mediating process in inter-agent activity to achieve common understanding and fulfil common goals. These models of *push* and *pull* are further elaborated in [15].

5. SYSTEM INTEGRATION

5.1 Introduction

Integrating the design results from HF, IM, interoperability, management, security and vulnerability is an immature engineering process. This process must also recognise that we are now building what should be regarded as 'living' systems, with rapidly changing users and user needs, different sociological models of how they are used, as well as the more obvious dynamics in their topologies of their use, placement and communications. This new dynamics of systems use, and systems acquisition and through use support is posing many questions that in the demanding environment of the military have not yet been properly answered.

5.2 Keys to the future

Architecture: It has long been the belief of systems developers, designers and those developing long term requirements that any future system must be built according to well understood and widely agreed architectural principles. Unfortunately at the higher levels of abstraction, systems are what are technically called 'soft'. They are not amenable to strong, or hard theorising. For JBD we are nonetheless developing a technical architecture, that is intended to inform both acquisition and commercial developers of military systems. The need here is for a System of Systems (SoS) architecture, and for its communications needs a network of networks (NoN). Such an architecture must also provide the ability to inter-work with national legacy systems and coalition systems.

Interoperability: A useful approach towards understanding interoperability is to evaluate interoperability matrices that relate different interactions between users, and then to quantify these interactions, in terms of need, service description, and finally in terms of the protocol and physical interface needs. This can be undertaken in both a technical and a cost-effectiveness sense. Major problems are that HF and IM are not mature, and the need to inter-work with legacy systems. The policy being advocated for legacy systems is to interface to a civil standard in the case of communications. For software the approach is to pursue a variety of interface options; CORBA object wrapping, the use of interface description language (IDL), and HTML interfaces (web pages) and examination of more powerful schemas based on semantic labelling concepts, using XML.

Systems and Network Management: It is now widely recognized that unless a SoS is in some sense manageable as a complete whole, then control of the system is likely to be lost in adverse or complex circumstances. This is being pursued by invoking a wide range of management capabilities in new systems, and by specific development of inter-system management interfaces. Although longer-term systems using agent based distributed management are attractive, they are unlikely to find application in military systems for some time, because of a lack of standards for these applications and security concerns. Whilst self-healing and self-adaptive systems are of course attractive, especially if a SoS becomes so large that its overall complexity is not within the conceptual grasp of a management function, the implications for denial of service and other security weaknesses demand much more research.

Security and Vulnerability: Security and vulnerability over a SoS poses many problems, notably the use of differing system security policies, different cryptographic and related boundary protection devices, different schemas for their management (placement, local and remote control, key management etc). This problem is difficult enough within a single nation, but when coalition interoperability is needed the difficulties are far greater. Difficulties arise due to the absence of common agreement on the architecture, processes, and the function and performance of boundary devices from different nations.

As a SoS, or a NoN, is expanded, increasing difficulties occur in management, in guaranteeing its security, and in both controlling and meeting the needs of the increasingly diverse community of users. The result is that vulnerabilities and shortfalls present in each system may become manifest over much wider domains and be easier for adversaries to exploit. The interfacing mechanisms themselves may also admit new vulnerabilities. These problems are an important part of the technology challenge for new C2 systems.

6. CONCLUSIONS

The provision of an integrated, readily protected CIS infrastructure that can provide a wide range of resilient services worldwide is far from straightforward.

The ready availability of a wide range of low-cost and powerful COTS products provides the apparent ability to build large powerful complex CIS. However our poor understanding of the human–machine inter-relationship, and the need to include human factors in a far more powerful way than is currently the case, remain substantial risks to the ambition of truly joint, truly seamless, and truly effective coalition command and control.

The provision of JBD, including coalition interoperation, requires not just technical solutions, but different management and procurement processes for its success. These are sociological issues of system-building, that are every bit as critical as the technical aspects.

We are now developing a more effective socio-technical systems-integration capability, that is bringing together the ideas of human information sharing and use, its control and communication by machines, and the man - machine relationship.

References

1. Montefiore, H., Enigma; *The Battle for the Code*, Weidenfeld and Nicolson, 2000.
2. Addison, D. and Fitzgerald G., *Information Systems Development: Methodologies, Techniques and Tools*, McGraw Hill, 1995.
3. Jarayaytna, N. *Understanding and Evaluating Methodologies*, McGraw Hill, 1994.
4. Stapelton, J., *Dynamic Systems Development Method*, Addison Wesley, 1997.
5. Sleigh, A. and Pratley, P. (Col); *'Achieving a Balanced Capability for Future Operations'*, June 1999, unpublished MoD paper.
6. Boynton, A. C. and Victor, B., *'Beyond Flexibility: The Dynamically Stable Organisation'*, California Management Review, 34/1, Fall 1991, pp 53-66.
7. McGahan, C., Fernall, R., and Campbell, J., *'Joint Battlespace Digitization Statement of User Needs Human Factors Benefits Analysis'*, October 1999, unpublished DERA paper.
8. Moffat, J and Prins, G., *'A revolution in military thinking? – issues from the 1999 DERA Senior Seminars'*, July 2000, Journal of Defence Science, Vol. 5, No. 3.
9. Hamid, S., *'Digitization – Human Sciences Research Strategy and Co-ordination Mechanism'*, March 2000, unpublished DERA paper
10. Davenport, T. H., *'Saving IT's soul: human-centred information management'*, March 1994, Harvard Business Review, pp 119-131.
11. Rooney, D.,*'Mission Command and Battlefield Digitization'*, March 1998, unpublished DERA paper.
12. Henderson, S.,*'Shared Situational Awareness in PJHQ Teams"* May 1999, unpublished DERA paper.
13. Bonner, M., Taylor, R., Fletcher, K. and Miller, C., *'Adaptive Automation and Decision Aiding in the Military Fast Jet Domain'*, unpublished DERA paper..
14. Black, U., *OSI: A Model for Computer Communications Standards*, Prentice Hall, 1990.
15. Davenport, T.H., *Information Ecology: Mastering the Information and Knowledge Environment,* Oxford University Press, 1997.

This page has been deliberately left blank

Page intentionnellement blanche