

COMPUTING



MINISTRY OF DEFENCE

This is one in a series of Information Sheets, on topics that are likely to be of growing importance to defence. It has been produced by a panel comprising some of the UK's leading experts (see box below)

ITS FUTURE AND ITS IMPACT ON DEFENCE

The Computing Technology Panel

In addition to MOD staff led by the Chief Scientific Adviser (CSA), the Computing Technology Panel comprised of UK and world leading scientists and engineers from industry and academia.

Professor Keith Burnett is Head of Atomic and Laser Physics at the Clarendon Laboratory, Department of Physics, University of Oxford, and has research interests in atomic interactions, ultra-cold atomic physics, quantum optics and quantum computing.

Professor Wendy Hall is professor of Computer Science in the Department of Electronics and Computer Science at the University of Southampton. She is currently an EPSRC Senior Research Fellow and has research interests in web technologies, knowledge management and agent-based computing.

Professor Cliff Jones is Professor of Computing Science at the University of Newcastle upon Tyne, he has worked in both industrial and academic software projects, and his experience is in formal methods and dependability.

Professor Roger Needham was formerly Head of the Computing Laboratory, University of Cambridge where he did research in systems, networks and security. He is now Managing Director of Microsoft Research LTD Cambridge.

Professor Ronan Sleep is Chair of Computing Science at the University of East Anglia and an invited Direct Entry Fellow of the British Computer Society. His current research interests include ambient intelligence and he helped formulate the ambient intelligence vision which is driving research in this field in Europe.

David Turek is Vice President of Emerging Technology at IBM Poughkeepsie NY, his current interests include 'grid computing' and the use of scaleable hardware and software to solve difficult scientific and technical problems.

Computing is already at the heart of defence

In this information sheet we are discussing a technology that is already at the heart of the UK's Defence, with software-intensive procurements running into billions of pounds in the pipeline. There are hardly any aspects of defence that do not now, or will not soon, depend on computing technologies:

- the collaborative development and maintenance of operational plans;
- analysis of Intelligence data, support to Intelligence Analysts, and dissemination of Intelligence reports;
- computer-assisted battle management and combat support systems in ships, on aircraft and on the battlefield;
- control of weapon systems - be they conventional, such as artillery, or the latest generations of intelligent munitions;
- the Ministry of Defence has a large requirement for business support software for Personnel Management, Office Automation and Logistics.

DEFENCE COMPUTING IS DRIVEN BY THE CIVIL MARKET

Since the silicon chip was invented the computing industry has progressed at a rate consistent with Moore's Law, with processor power and memory capacity doubling every eighteen months. All attempts by the defence market to produce bespoke computing solutions have quickly led to systems that massively under-perform what cheaper commercial technology can provide. As an explanation of MOD's inability to buck the market, you need look no further than the size of its research budget. MOD spends £450 million per annum on research into all non-nuclear technologies. Microsoft spends more than \$1.4 billion per annum just on software research and development.

In looking at the future of defence computing, we have to look at the future of the civil computing industry. The first thing to say is that some key segments of the industry have started to cool down. For the first time, in 2001, the sales of personal computers (PCs) declined. This, coupled to the decline in mobile phone sales, has reversed a non-stop period of growth in the volume of silicon chips sold that has lasted over twenty years. It is also clear that there have been few if any fundamental technical advances within computing in the last five years. It is, however, likely that there will be a massive growth in the market for computing appliances, or so called 'Ambient' or 'Pervasive' computing. In contrast to PCs, these will be cheap, fixed functionality, mass-market devices, such of those supplied by satellite and cable TV broadcasters, or carried around as personal digital assistants. The trend now seems to be that the major advances in the computer industry will be driven by the novel application of computers to the way we live our lives, rather than the ever-increasing capability of computers in general, and PCs in particular. For this reason, the reader may be surprised at the lack of coverage of new technologies that promise faster digital computers. The panel feels it is the application of the existing capabilities of computers that will excite the market, and which will also offer the greatest possibilities for enhancing defence.

MOD IS DIFFERENT FROM OTHER ORGANISATIONS

At one time, MOD thought it was so different from other organizations that it was justified in buying bespoke computer systems. Those days are long gone and the bulk of MOD's computer systems now comprise Commercial Off-The-Shelf (COTS) technology. There was

however some truth in MOD's belief that it was different, and, as a consequence, much of MOD's Information System R&D expenditure now goes on adapting COTS technology to some of the defence-specific applications MOD has.

Harsh Physical Environments- In ships, submarines, aircraft, tanks, other land vehicles and carried by soldiers, COTS technology faces a physical environment that is potentially far more hazardous than portable computers normally face:

- electromagnetic radiation from our own equipment, and deliberate jamming from our opponents;
- physical shocks, e.g. from depth charges in a submarine;
- temperature ranges from arctic to desert;
- nuclear, biological and chemical contamination/decontamination;
- humidity, dust and water.



Computers are at the heart of all logistics operations and scheduling. Although the deployment and reach of supplies is much further than most civil applications there are commonalities between MoD's objectives and those of commercial supply chains.

Security- MOD's security needs differ significantly from commercial organisations. The top levels of confidentiality require far greater protection and for longer periods of time than commercial organisations would ever need. MOD faces the possibility of cyber attacks which may be far more sophisticated or violent than other organisations face. In addition, MOD has many more levels of security classification than most commercial organisations would need to use.

Ability to handle change- MOD's procurement processes are geared to buy equipment that will often have a service life of decades. When purchasing computer equipment that becomes obsolescent in a matter of a few years, MOD obviously faces great challenges. Sometimes the fact that computing equipment becomes obsolete does not matter provided it still does the job, and MOD can buy a lifetime supply of spares. More often, MOD will be forced to upgrade computer hardware and software many times during the lifetime of a piece of equipment.

MOD also has to face the fact that it must procure computer systems that can support a wide range of often unpredictable operational scenarios. Operations now vary from humanitarian, to peace enforcement and to peace keeping, whilst the safety of the UK requires that MOD retain the capability for high-intensity warfare against a capable opponent. Even within a single operation the intensity may escalate suddenly, or the intensity might gradually decline from peace enforcement to peace keeping. Few commercial organisation face such diversity and unpredictability in the business requirements that their computer systems must support.

Putting the engineering into software engineering

The days of the amateur programmer are perhaps coming to an end. Software will become more dependable and software development will become more predictable for a number of reasons:

- software development processes are maturing;
- reusable software components are (painfully slowly) becoming a reality;
- software programmers are becoming better trained and more professional;
- organisations are starting to apply best practice to software developments.

The UK has long been a world leader in applying formal (mathematical) methods to software development. Until recently, this has been seen as a high-cost approach only suitable for small safety-critical software components. Formal approaches are now starting to become mainstream techniques to assist the

development of large, dependable software systems. In the future we would perhaps like such systems not only to be dependable but also to evolve as the future environment changes. The concept of achieving a dependable system that has evolved from the designer's original is, however, a formidable challenge.

Developments of dependable software systems are potentially of great significance to MOD. MOD has a growing number of computer-based systems that are either safety-critical, or mission-critical. Rigorous software engineering techniques will be needed to implement such systems. MOD's requirements to develop complex safety and mission critical systems tend to push the commercial state-of-the-art beyond that which is widely needed in industry, and as a consequence MOD has invested in the development of scaleable techniques for critical systems.

Interoperability and open standards

Increasingly, organisations are using the Internet to interact with external bodies - be they customers, suppliers or partners. There is a strong parallel here with MOD's desire to operate in coalitions with the armed forces of other countries, and with non-governmental organisations - such as humanitarian aid. In contrast to corporate Intranets, communication with external bodies means that you have to interoperate with organisations over whose computer systems you have no control. Software has long been so complex that the principal mechanism for achieving interoperability in Intranets has been for organisations such as MOD to standardise on a few dominant software products. This is a much less viable option when trying to interoperate with external organisations, because it is seldom possible to be sure that external bodies are using the correct version of a particular software application. As a result, external interoperability tends to be the preserve of open, non-proprietary protocols, such as those that underpin the development of the Internet. At the moment, open standards tend to be limited to publishing data. With the development of standards such as XML (eXtensible Markup Language), these standards will expand into publishing structured information, sharing information and sharing services.

A lack of interoperability has been the key problem that has prevented MOD producing an integrated capability from the "system of systems" that it owns. In the past few years research into techniques to support the "system of systems" has dominated MOD research spending, under the Joint Battlespace Digitization Initiative, and more recently Command and Battlespace Management.

Open Source Software

The Internet has also seen the rise of a new force in the industry - the Open Source (free) Software movement. It seems incredible that software, which is often developed by volunteers, whose source text is freely available, can be as robust and reliable as proprietary products that have received massive commercial investment. The combination of Open standards and Open Source reference implementations may be spearheading a move towards a computing industry that will be less dominated by a few large software vendors.

Open Source is generating a debate in MOD about the most fruitful approach to exploiting the results of MOD's research into computing. A recent Defence Scientific Advisory Council (DSAC) report went so far as to suggest that Open Source should be the default mechanism for exploiting MOD-funded software research. However, research using Open Source Software design methods often leads to knowledge of how something can be achieved rather than a perfect piece of software.



Computer simulation is a valuable tool in training and mission planning. Advances in hardware and software driven by the commercial sector have led to very realistic and accurate synthetic environments and simulation tools.

Interfacing computers and humans

As the focus of industry investment moves from faster, more functional component technologies, towards the application of computers in people's lives, the human/computer interface is becoming a major limiting factor. As a consequence, technologies to facilitate better interaction between computers and humans are attracting major investment:

- new technologies for larger, more portable, less bulky, more robust, lighter, higher resolution, cheaper, less power hungry displays;
- advanced visualisation techniques such as Virtual Reality;
- software agent technology to allow more intelligent interfaces and tools for construction

of complex internet systems;

- speech recognition;
- gesture and facial expression recognition.

MOD will be able to utilise these developments for better information presentation to commanders, improved mobile displays, interfaces for hands-free situations, and advanced training simulators.

Many little ones beat a big one

High-end computers are increasingly moving towards very large clusters of low cost computers. There is a lot of effort going into squeezing as many computers as possible into as small a space as possible. Such computers are referred to as "Blades". There are also moves to join up clusters of existing computers over the Internet to create a concept of a virtual mainframe computer called "the GRID". Blades and the GRID are part of a movement that is providing new, cost-effective approaches to high-end computing.

Blades and the GRID highlight the interplay in the software industry between advances in hardware and software development. Conventional super-computers are just very fast computers that have a single sequence of computer instructions that execute *very quickly*. In Blades and the GRID there are many computers working on the problem at the same time. This means that an algorithm that executes very fast on a conventional super-computer may not be suitable for distributing over a large number of low-cost computers. Fortunately, many computationally intensive problems are amenable to distribution over many computers working in parallel - but new algorithms often have to be developed for this parallel-computing paradigm.



Command, Control and Information Infrastructure blurs the distinction between communications and computing technologies. The merging of these two technologies is increasingly taking place in the civil sector as well, as Personal Digital Assistants (PDAs) handle both voice and email correspondence, and computers are linked by a variety of wire and wireless/radio communications to the internet and intranet. (See the Information Sheet on 'Communications and their influence on the battlefield').

Solid-state non-volatile storage

It is remarkable how long the ubiquitous disk drive has remained the dominant technology for storing data files. Newer technologies for solid state data storage are now emerging in the portable computing appliance market.

An emerging technology at present is flash memory, which is used for example in the memory cards of consumer digital cameras. It has a slow write speed, and can only be erased in complete blocks, so it is not a replacement for general purpose computer disk drives, but is usable as a disk replacement in some consumer devices. It also has a limited number of write cycles, of the order of 10^5 . Two new technologies are potentially important. Ferroelectric memory uses a special dielectric in the storage capacitor of its cell. The read and write speeds are expected to be comparable to the solid state RAM used for computer memories, and individual bits can be over-written. The cells are somewhat larger than in other memory technologies, and the materials are very challenging, but it could potentially be used for the main memory of a computer, giving a persistent store and no need to reboot, which will make it ideal for some portable computing devices. MRAM uses magnetic materials to store the data and spin dependent tunnelling to read it out. The cell size is very good, and the data access speeds are excellent. It is suitable for use as replacement for both the main memory and disk of computers. Trial commercial production is due to start in 2003.

In time, these technologies could start approaching gigabyte capacities and they are orders of magnitude faster than conventional disk drives. A disruptive technology if we have ever seen one!

Given MOD's need for robust, mobile computing devices, a replacement for disk drives has great attractions for use in aircraft and on the battlefield.

Knowledge is the key to competitive advantage

The Internet and corporate Intranets are awash with data. How can organisations extract the valuable nuggets of information from this sea of data? A number of research areas could dramatically increase the value of the information extracted:

- Natural Language Processing allows computers to analyse the meaning of text. If computers can understand the meaning of text either linguistically, or using sophisticated statistical methods, then information searches can be much cleverer.
- Data mining techniques use advanced analytical algorithms to spot trends and patterns in large data sets.
- Metadata allows the structure of data to be made explicit. For example, metadata could be used to

distinguish the author, creation date, revision history, headings and subheadings, references, etc. of a document. Once metadata is used to describe the structure of data, it is much easier for search engines to query the data intelligently.

It is widely recognised that the quality of Military Intelligence is a key to prevailing in a conflict. As more and more Intelligence data is digitised, MOD will gain increasing benefit from applying state-of-the-art Information Management technology.

MOD now recognises that the deployment of armed forces is just one dimension of modern conflicts. The outcomes of today's conflicts are often as much to do with public opinion in the UK and abroad, as they are about deployment of our armed forces. As a consequence, issues such as Press relations and the associated Information Management Technology can be critical to the successful resolution of a conflict.

There is a linkage between armed conflict and the wider issues of Public Relations. MOD accepts a duty of care to minimise civilian casualties and casualties amongst our forces and those of our Allies. Better Intelligence (strategic and tactical) is the key to minimising avoidable casualties.

Quantum computing

Computing has made progress thanks to certain milestones in technology (valves to transistors, transistors to integrated circuits, magnetic tape to hard-disk drives etc). One of the technologies to attract most press attention is quantum computing. Working at the massively counter-intuitive quantum level of physics, a quantum switch takes advantage of a quantum effect called superposition to take a multitude of states simultaneously. See the box on Quantum Computers on page 7. Have any of the previous new computing paradigms succeeded in displacing the humble silicon chip? - No. Will quantum computers succeed where all the others have failed? - Not soon. The timescales for development of Quantum Computer technology are far longer than conventional improvements in the technology we have around us today. There are numerous technical problems of the most challenging kind to be solved before a practical quantum computer is possible. Why try? In a word it is code cracking - quantum computing is one of the very few ways that anyone can imagine that modern cryptography can be cracked by brute force.

Other alternatives to silicon are being researched such as biological and optical computers. These are unlikely to ever significantly dent silicon's market dominance but may well find niche uses that well match the properties of the new technologies. It is clear that future computing technologies, biotechnology and nanotechnology will go hand in hand as technology develops. See the Information Sheet on NANOTECHNOLOGY: ITS IMPACT ON DEFENCE AND THE MOD 05/02/2001.

FUTURE BENEFITS TO MOD

One achieves success in conflict (armed and political) by:

- having superior intelligence information;
- making better decisions than your opponents;
- reacting faster;
- being able to bring overwhelming force to bear;
- applying force more precisely;
- communicating your political message more effectively.

Computers and communications are key to all these factors. Digitised information flows faster, can be analysed more quickly, and can be presented more effectively. Computers and communications will be, and indeed already are, at the heart of the UK's ability to achieve its political and military objectives.

Computers are already allowing the UK to "do things better". We can manage conflict in the ways we have always done, but faster, smarter, and making fewer mistakes. Increasingly, the challenge is to "do better things". Using computers we can find new ways to confuse and disorient our enemies, find new sources of intelligence and use the resources at our disposal much more effectively. Future conflicts will be won or lost by the ways we collect and exploit the information at our disposal. Not surprisingly, MOD seeks what it calls "information dominance" - and information processing is the realm of computing.

The technology MOD uses will come from the civil market, but no organisation uses it as the MOD will use it, given the extreme physical conditions that MOD faces, and the sorts of physical and electronic attacks that MOD will face. MOD will never again be a driver of computing technology, but it faces massive research problems in deploying commercial technologies within its own unique circumstances.

THE MOD RESPONSE TO COMPUTING

Within the MOD, computing research is funded through the Applied Research Programme (ARP) and the Corporate Research Programme (CRP).

The ARP currently focuses on the integration and interoperability of COTS technology in the system of systems that comprises Command and Battlespace Management. This application of computing will address the full range of MOD's operational processes, including:

- strategic, operational and tactical planning;
- strategic and tactical Intelligence analysis and dissemination;
- Logistics;
- Command and Control;
- embedded systems in military platforms (armoured fighting vehicles, ships and aircraft);
- smart weapon systems.

This will remain the main focus of MOD expenditure, and will utilise many of the developments in computing that are described in this Information Sheet. This ARP work feeds directly through into military doctrine.

The ARP also researches the military differentiators, particularly security, where MOD will maintain its expert customer status.

Because of the dependence on COTS technologies, MOD will continue to refrain from research in the underlying components of computing technology, and will concentrate on funding the application of COTS technology to defence. Both the ARP and CRP will continue to fund a wide-ranging Technology Watch of emerging computing technologies.

MOD will need to expand its research into adaptable computing architectures and techniques to ensure that future MOD computing systems can better adapt to the extreme range and dynamics of the operational scenarios it will face in the future. MOD will have to accept the fact that technology alone cannot meet this challenge, and MOD will need to continue to drive forward changes to its procurement processes.

Within the CRP programme, MOD will continue to support research into safety and mission critical systems, as well as researching the military applicability of leading edge computing technologies such as coherent electron devices and single photon detectors and emitters for quantum computing and nano-electronic and organic semiconductor devices.

To best exploit the results of its research, MOD will increasingly publish its research software as Open Source either on the Internet, or to the more restricted defence community.



PRISM: A prototype computer based tool to track and log medical symptoms on the battlefield. Information tools on the battlefield, such as PRISM, will lead to improved support and effectiveness in operations and conflict situations.



The use of networked or 'grid computing' to solve large problems and cope with large resource needs is something the Internet Service Providers have embraced rapidly. Grid computing networks a very large number of low cost

computers into 'Blades' to enable very powerful systems to be configured. The future use of the internet will give us virtual mainframes providing a cost-effective high-end computing resource.

QUANTUM COMPUTERS

To explain how a quantum computer works, it is useful to consider first how a conventional computer operates. The 'language' of current computers is based on representing numbers; letters and symbols by a series of zeros (0) and ones (1). Each 0 or 1 is called a bit. To uniquely identify a single character such as a letter of the alphabet requires 8 bits, which together is called a byte. For example, the 8-bit byte that represents the letter "a" in a computer is 01100001. Since computers are electronic devices, they use voltage levels to represent the 0s and 1s; typically a level 0 means a voltage below 0.4V and a level 1 means a voltage over 3.5V.

Most of the world about us can be explained in terms of what is called 'classical' physics. However; devices that operate at the atomic and sub-atomic scale are governed by 'quantum' physics. Quantum physics shows us that at these very small scales, the behaviour of particles is governed by special properties call quantum states or numbers associated with the particles.

In quantum computing, the byte is replaced by a single element called a qubit. A qubit is in effect a single entity rather like a conventional computer's bit, but actually it is a combination of many quantum states of atomic or sub-atomic particles. Consequently, in a single qubit it is possible to carry lots of 0s and 1s all together but in a single quantum bit (hence the word qubit).

The process that enables all these quantum states to be carried as one entity is called 'entanglement'.

Since quantum physics is not as intuitively logical as classical physics, its concepts are more difficult to explain. However, by way of a rather simple analogy, imagine a picture on a conventional computer of the 'Mona Lisa'. The picture of the 'Mona Lisa' is stored in the computer as many millions of bits. However, if somebody talks to you about the 'Mona Lisa', by just hearing the name, you know what the picture looks like without having been given the enormous string of 0s and 1s that the computer needs to re-draw it. In the same way, in a quantum computer, the qubit is the equivalent of the name 'Mona Lisa'. Of course you can visualise the 'Mona Lisa' because you have a memory of what it looks like. The quantum computer equivalent is the means to 'untangle' the information buried in the qubit.

Consequently, quantum computers have the potential ability to carry and process large amounts of information in parallel and at very high speeds. It is for this reason that it is believed that they could be useful in dealing with the most computationally intense tasks, such as code breaking.

The key problem facing quantum computer developers is the one of finding a suitable quantum register, which can not only be set-up with the correct input data but can be manipulated with quantum operations, without the states within the computer decaying and information being lost. Unlike the reliability of conventional digital logic, most quantum logic can be somewhat error prone.

CONTACTS

If you have any queries on this information on this information sheet or its contents please contact:

Director of Technology Development, MOD,
Metropole Building,
Northumberland Avenue,
London, WC2N 5BP

The Beowulf network of PC's on page 7 was built by Don Becker,
picture is courtesy of Michigan Technical University

