Australian DEFENCESCIENCE

Winter Issue Volume 16 Number 2 2008

Clothing test with mobile mannequin

Clones that counsel

New coatings

Communications security

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Australian Defence Science. Volume 16, Number 2**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Australian Government,Department of Defense,Defense Science and Technology Organisation,Australia,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

CONTENTS

Australian Government

Department of Defence
Defence Science and
Technology Organisation

The Defence Science and Technology Organisation (DSTO) is part of the Department of Defence and provides scientific advice and support to the Australian Defence Organisation. DSTO is headed by the Chief Defence Scientist, Dr Roger Lough, and employs about 2200 staff, including some 1300 researchers and engineers. It is one of the two largest research and development organisations in Australia.

Australian Defence Science is published quarterly by DSTO Defence Science Communications. Unless labelled copyright, material may be reproduced freely with acknowledgement.

Managing Editor: Jimmy Hafesjee
e-mail: jimmy.hafesjee@defence.gov.au

Editor: Tony Cox
Phone: 61 8 8259 6554 Fax: 61 8 8259 6191
e-mail: tony.cox@dsto.defence.gov.au

Media enquiries: Lorraine Mulholland
Phone: 61 2 6128 6385
e-mail: lorraine.mulholland@defence.gov.au

Mailing list enquiries: Angie Toutziarakis
Phone: 61 3 9626 7432
e-mail: angela.toutziarakis@dsto.defence.gov.au

More information is available about DSTO on its web site at: www.dsto.defence.gov.au

ISSN 1441-0818

Mobile clothes horse to test protective suits

DSTO has recently acquired a mannequin system with human-like motion capabilities for putting chemical biological radiological (CBR) protective clothing and equipment to the test in simulated conditions.

Previously, testing clothing for protective qualities against CBR effects relied mainly on checking samples of fabric rather than the garment as a whole when being worn.

This form of limited testing, crucially, does not take into account the performance of garment closure devices, such as Velcro fasteners, zips, buttons and buckles, and the fit of the garment design on the human body when in movement, plus the fit of the garment when in use with other protective equipment such as a respirator.

According to DSTO researcher Rebecca McCallum, these factors can significantly affect the degree of protection provided to the wearer. "The use of an articulated mannequin that can perform a realistic range of movements enables us to study the protectiveness of this clothing and equipment much more thoroughly," she says.

A set of mannequins ready to go

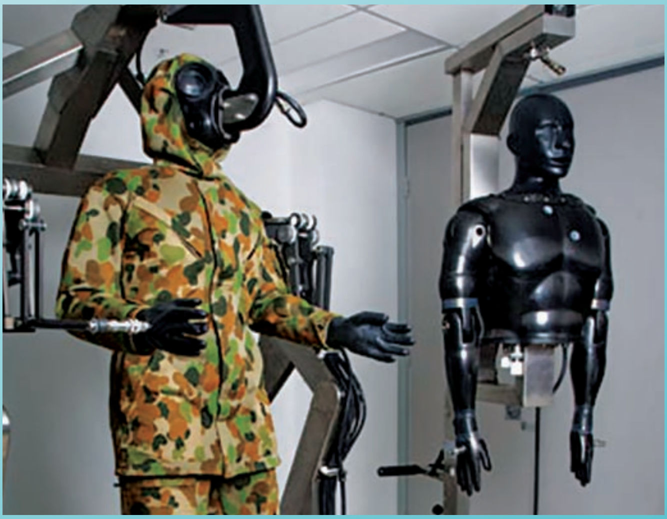
The mannequin ensemble consists of a full body mannequin, and a separate torso and head unit.

The mannequins can be programmed with movement sequences that are representative of any user group's expected activities within a CBR environment in order to realistically simulate the stress placed on individual protective equipment (IPE) closures.

The full body mannequin is used to measure the performance of protective equipment during simulated activities such as walking, jogging, running, squatting, lifting, carrying, sitting, and reaching.

Since this mannequin, however, is attached by the head to its supporting frame, it is unable to replicate exaggerated movements of the head and neck.

The full-length mannequin in Army CBR uniform being put to simulated work.



The fully mobile full body mannequin and the head and torso unit.

Test functionality for these aspects of movement is therefore provided instead via the torso and head unit, which is mounted from the waist up on a frame that can move the limbs, torso and head in several planes simultaneously.

"Having this extra mannequin with a fully-articulated neck allows us to test the integrity of respirator and hood interfaces of protective ensembles – a key area of the body that requires high levels of protection," says McCallum.

Cutting-edge technology to keep humans out of harm's way

DSTO's mannequin ensemble, only the second of such in existence worldwide, was made on commission by UK animatronics company Crawley Creatures.

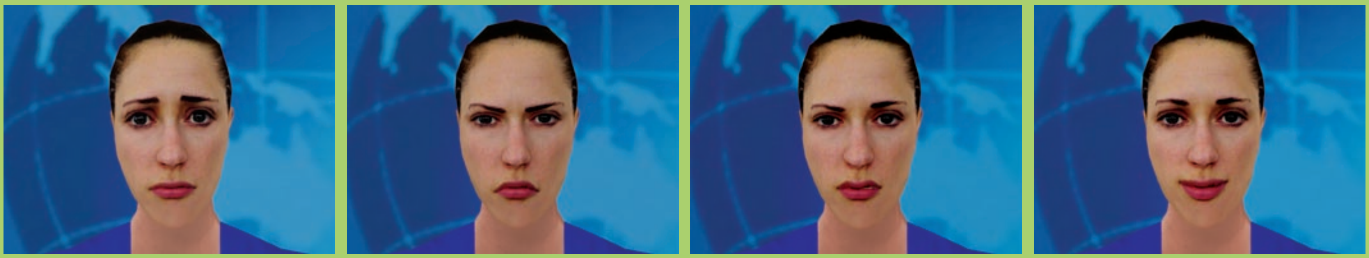
The motion-simulating mannequin system was developed specifically for CBR testing by Defence Research & Development Canada with the assistance of Crawley Creatures over the period of two years. Access to the mannequin technology was made available to Australia through The Technical Cooperation Program (TTCP).

As part of facilities development for the CBR research program, a new environmental chamber is to be built at DSTO Melbourne where the mannequin ensemble will be housed, and where testing of the IPE equipment will be undertaken.

The information gained from testing will assist in the process of selecting protective equipment for the ADF, and help determine the levels of protection provided by various IPE items.

The protection factor data gained will then be used in operational analysis modelling to better predict the capability of Australian Defence Force units to maintain operations in CBR-contaminated environments.

Clones that counsel



Different facial expressions of Virtual Adviser, 'Jane':
L - R, afraid, angry, contempt, happy.

Information overload is a growing problem for military decision-makers. Personnel under pressure can now assimilate information by using virtual persons with human-like expressive capabilities.

In the current age, information is abundantly available via media such as the internet, mobile phones, and various other forms of information technology connectivity coming into widespread use.

However, an increase in the amount of information a person receives often fails to correspond to an increase in understanding.

DSTO is seeking to establish better ways of managing and delivering information. One means of doing so is to apply information sorting systems with semantic and reasoning capabilities, and a further such measure involves the use of computer-generated characters displayed on screens, known as Virtual Advisers, that communicate information directly to human decision-makers with speech and gestures.

The content delivered by Virtual Advisers may be either human-authored, or generated through an automated extraction process, and it may also be annotated with identifiers to cue what is to be spoken and how it is to be expressed.

A better means of information delivery

"The advantage of Virtual Advisers," says DSTO researcher Dr Steven Wark, "is that they can deliver context-rich forms of information, such as those contained in maps or diagrams, in a very natural way. Having this capability, they provide an alternative to the use of valuable command staff for information delivery. What's more, Virtual Advisers are portable, they don't get tired, and you can call on them anytime!"

The Virtual Adviser characters can be combined into a team of presenters, with different members being associated with different kinds of information or domains of expertise. Each Virtual Adviser is given the floor separately through display management processes, depending on which has the most relevant information at any particular moment.

The Virtual Adviser briefing process is also being made interactive. The aim is to allow humans to ask the Virtual Advisers questions, and for the Virtual Advisers to respond similarly with speech, made possible by speech recognition and natural language processing software.

Virtual persons with a compellingly human face

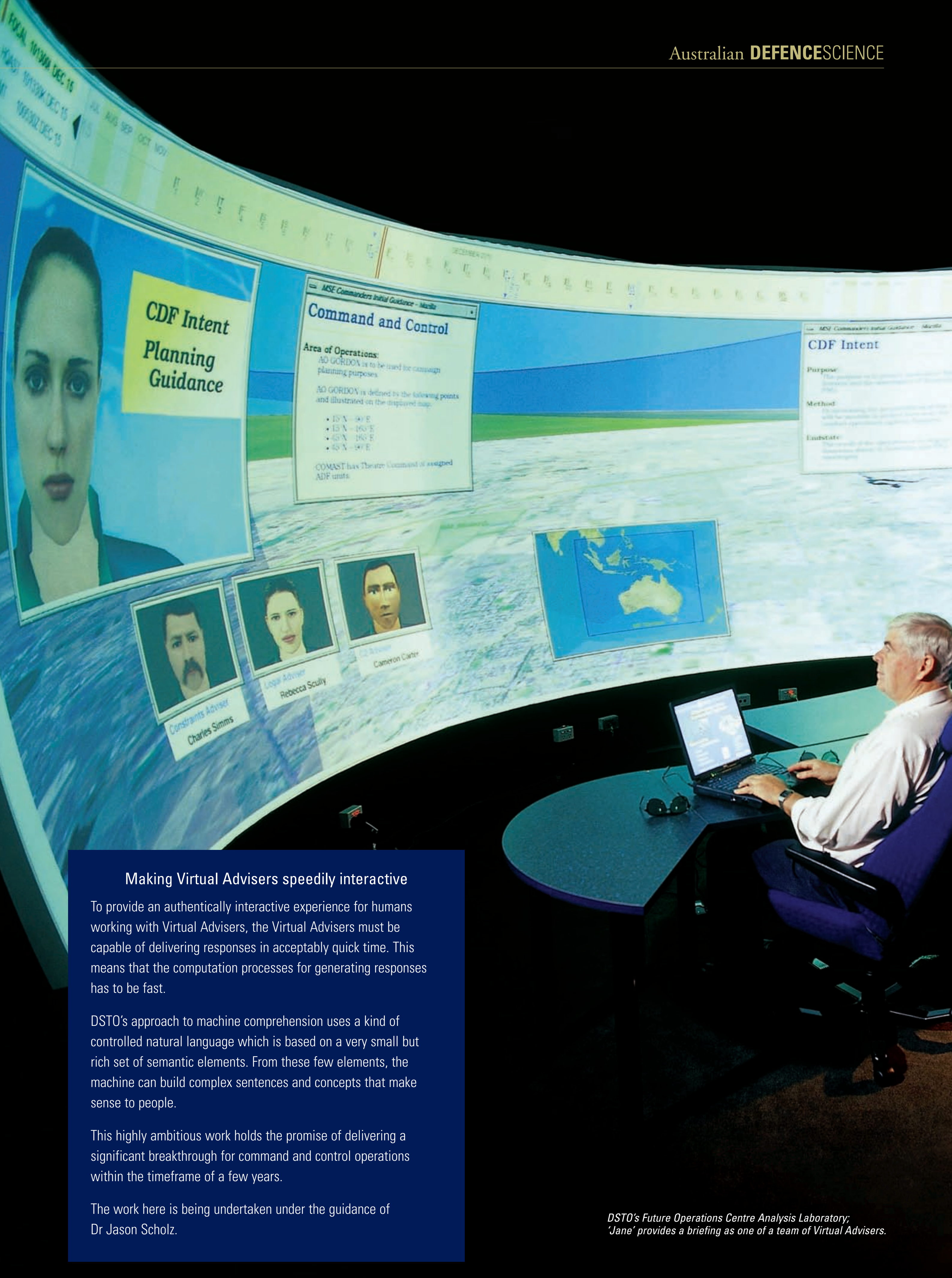
Further enhancing the Virtual Adviser's human-friendly nature, recent technological advances have enabled these characters to automatically generate facial expressions and gestures to convey degrees of confidence, urgency and importance when speaking.

Experiments conducted by DSTO and the University of Adelaide have shown that different facial characteristics displayed by a speaker will influence a user's affective trust, implicitly imparting uncertainty to the user if required, which at times can be a vital form of qualification for any information delivered.

"According to a recent experiment," says Dr Wark, "recall of information delivered by Virtual Advisers is comparable to that delivered by human advisers."

To further their use for military purposes, Virtual Advisers are being integrated with DSTO's Virtual Battlespaces as part of the Coalition Distributed Information Fusion Testbed. They are seen as having a vital role to play in assisting with today's network centric warfare approaches to operational decision-making.

The Virtual Adviser technology is also regarded as having potentially widespread application in civilian areas such as commerce, transport, security, law-enforcement, mining, health care, emergency services and education.



Making Virtual Advisers speedily interactive

To provide an authentically interactive experience for humans working with Virtual Advisers, the Virtual Advisers must be capable of delivering responses in acceptably quick time. This means that the computation processes for generating responses has to be fast.

DSTO's approach to machine comprehension uses a kind of controlled natural language which is based on a very small but rich set of semantic elements. From these few elements, the machine can build complex sentences and concepts that make sense to people.

This highly ambitious work holds the promise of delivering a significant breakthrough for command and control operations within the timeframe of a few years.

The work here is being undertaken under the guidance of Dr Jason Scholz.

DSTO's Future Operations Centre Analysis Laboratory; 'Jane' provides a briefing as one of a team of Virtual Advisers.

New coatings for difficult and delicate surfaces

Many surfaces on today's military platforms and equipment are problematic to coat. Some of the new-generation materials being used are soft and fragile, and often also highly flammable. DSTO is devising new forms of paint and coatings for these hard-to-deal-with materials.

The coatings applied on Defence assets are highly complex mixes of materials purpose-designed for enhancing survival against both military threats and environmental stresses.

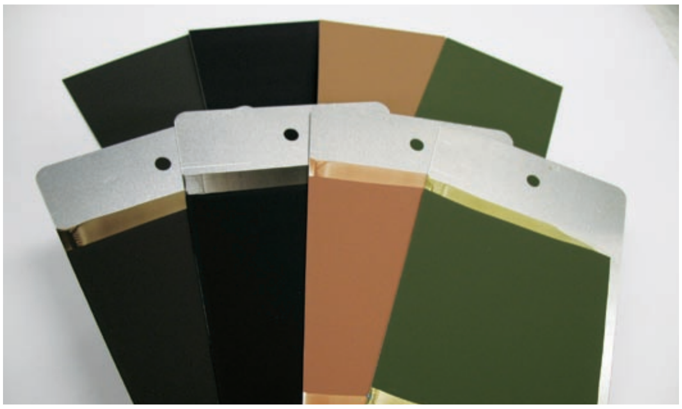
Militarily, coatings offer the benefit of reducing the visibility of an asset to enemy eyes through camouflage colouring that makes it harder to detect optically. Their textural composition can reduce the asset's visibility to infrared and radar sensors.

At the same time, coatings protect against structural degradation problems such as corrosion, thereby minimising the costs of asset ownership and maintenance – a major consideration for Australian Defence Force (ADF) operations.

The compounds used in military coatings are similar to those in specialist auto finishes, but have the added distinction of being able to dry to a hard finish without being baked.

A further aspect of their uniqueness is that the colours required for Defence purposes are, in general, completely different to those used in other contexts.

The military colour range includes tans, red and yellow ochres, olives and neutral greys in various shades for land assets, and greys with tints of blue and green suitable for sea and air assets. Similarly, gloss levels range from semi-gloss to completely matt finishes that ensure sunlight reflections and glint are minimised.



Swatches of DSTO's new waterborne coatings for the Black Hawk helicopter, with the required colour standards lying on table.

Above: a fire-resistant waterborne coating with high flexibility.
Top photo: DSTO researcher testing the spray application performance of waterborne Light Grey for the F/A-18.

Performance shortfalls with existing coatings

Highly developed though such coating formulations are, some limitations in capabilities have been identified.

One concerning problem is the cracking and peeling of brittle paint under conditions of high vibration – a particular problem on helicopters – resulting in exposed metal surfaces that are prone to corrosion. Another issue is the less-than-optimal ability of colour and gloss attributes to cope with Australia's harsh climatic conditions, with many reports of colour change and gloss instability requiring investigation by DSTO.

Improvements to coating performance are seen to be desirable or necessary in terms of flexibility, corrosion protection, chemical resistance and durability, all of which need to be attained without compromising existing properties of adhesion, camouflage capability and resistance to heat and humidity.

Meanwhile, Defence is also looking to develop coatings that are safer for personnel to apply. Such coatings can then replace existing kinds that contain hazardous compounds like chromates and isocyanates applied in organic solvents. A second broad aim is to formulate paints that are less polluting and free of toxic materials.

This work is being undertaken in several stages. One of the most difficult steps here, seen as requiring considerable ingenuity to circumvent, involves the formulation of high-tech paints using water as the primary solvent.

More effective safer-to-apply coatings

DSTO scientist Dr Christopher Lyons has been undertaking research on specialised water-borne coatings using some of the newest chemical technologies available today.

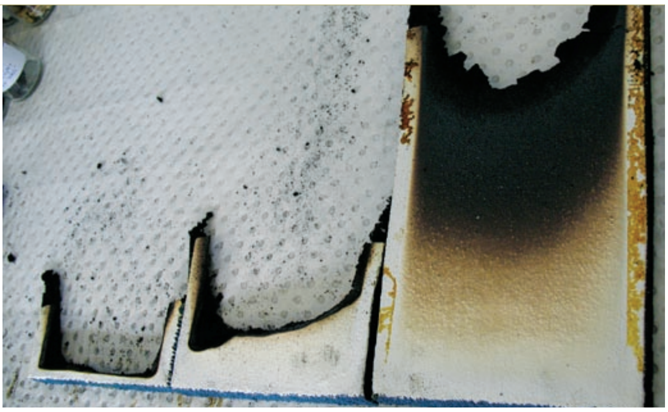
The products he has developed include waterborne topcoats resistant to chemical agents in colours of tan, olive drab and black for Army platforms, flexible waterborne topcoats for helicopters such as the Black Hawk, and waterborne coatings for RAAF applications with better chemical resistance than commercially available high-solids aerospace coatings.

Dr Lyons has also worked on paints for topside application on Navy vessels, having developed a colour-stable low solar-absorbing (LSA) pigmentation formula in the Storm Grey colour used on RAN platforms. This new pigmentation, which has recently been commercialised, solves the current problems concerning colour instability with existing LSA paints on Navy vessels.

The most developmentally advanced of the waterborne coating applications at present is a series of waterborne topcoats being formulated for RAAF platforms such as the F/A-18, with trials being planned for early 2009.

"The new RAAF coatings offer much improved flexibility over existing solvent-based coatings, thereby reducing problems with paint cracking on aircraft," says Dr Lyons.

"Being water-based, emissions to the environment are greatly reduced, yet their resistance to lubricating fluids, motor oil and jet fuel is measurably better than high-solids coatings. Also, these paints dry more quickly, so job turnaround time is very short, enabling aircraft to be returned to service sooner."



Aftermath of fire resistance testing for sample coatings, with best performing sample on right.

His current work involves fine-tuning the spray application properties of these paints so that RAAF painters can apply them to aircraft with minimal problems.

Flame retardant coatings

Another challenging problem that Dr Lyons has taken on in this area arises from the increasing use of polymers and rubbery materials in modern military aircraft construction.

"These soft fragile materials can be very flammable, and some of them are porous and extremely flexible," he says.

"However, the commercially available coatings that provide coverage for flexible materials don't generally have a fire retardant capability.

"Meanwhile, most of the fire retardant coatings commercially available are either hard and brittle, or aren't sufficiently viscous to coat the surfaces of porous foams without sinking into them," he explains.

Dr Lyons has been working in recent years to develop a coating that is both flexible and fire retardant. This has involved studying the fire retardant properties of various prototype coatings.

The testing process: trial by ordeal

To test their resistance to fire, the sample coatings are exposed to the blisteringly fierce glow of a radiant heat panel.

Each of the sample surfaces is angled with the top edge of the sample closest to the heat panel, so that when ignition eventually occurs, it begins at the upper edge of the sample, with the flame front generated moving downward.

The speed at which the flame front progresses is one measure of the fire retardant properties of the coating. Other measures include ignition delay, reduction of temperature rise and the capacity of the coating to extinguish the fire once started.

The prototype coating formulation produced as a result of this development process offers a balance of properties difficult to achieve with other products.

The next stage in this project will be to undertake in-service testing of the new fire retardant paint on a RAAF platform at some point in the near future.

Thinking ahead, Dr Lyons speculates, "With new kinds of raw materials being developed by chemical suppliers for these kinds of applications all the time, the possibility for improvements in coatings performance seems endless."

Protecting GPS information against disruption

This page and next: CRPA trials being conducted by DSTO at Woomera in late 2007.

Satellite signals that provide crucial information about place and time can be tenuously thin on arrival at end-user antennas. DSTO has been exploring ways of ensuring the signals are not disrupted.

Defence operations these days place heavy reliance on the Global Positioning System (GPS) when military units need to determine where they are, and how fast they are moving. The GPS technology also provides an accurate time reference to sub-second precision that enables units to precisely coordinate actions over great distances.

The signals received from this globally networked satellite navigational and time keeping system, however, are very vulnerable to disturbance by emissions from sources that are deliberately designed to create interference as well as those that inadvertently do the same.

Such vulnerability may pose a threat to Australian Defence Force (ADF) operational viability, as it also does to a range of crucially important civilian users of the GPS technology.

DSTO researcher Dr Chris Baker says GPS receivers can be rendered ineffective with simple, inexpensive, pocket-sized jammers made for this purpose, and also by signals emanating from radars, communications towers and TV network antennas that unintentionally have this effect.

"Therefore, we at DSTO continue to work on improving methods to counteract these forms of interference."

Safeguarding GPS signal integrity

To protect individual ADF platforms against GPS signal disruption, one solution being applied is an electronics system called the Controlled Reception Pattern Antenna (CRPA).

"The way in which a CRPA system defeats jamming signals or interference," explains Dr Baker, "is by receiving signals from all directions, and ignoring those from certain directions that are recognised to be aberrant.

"To enable testing of the efficacy of CRPA systems, we built jammers that emit jamming signals on the GPS frequency. When testing these antennas, the jammers are placed all around a CRPA in order to induce jamming stresses."

A series of trials has recently been carried out to compare the performance of the current-generation CRPA system, the GPS Antenna System-1 (GAS-1), with the next-generation CRPA system, the Advanced Digital Antenna Production (ADAP).

The CRPA trials

A two-stage trial was undertaken with the GAS-1 and ADAP systems fitted to an Army Black Hawk helicopter in late 2007 and on a Navy Seahawk helicopter in April 2008.

The CRPA systems were shown to perform beyond specification even in the presence of high jamming multipath and modulation effects caused by the rotating blades of the helicopters.

Meanwhile, DSTO carried out trials in May 2008 on board Navy ships to investigate a major problem involved in applying CRPA system anti-jamming protection on these platforms; this being the multipath emission reflections that ship superstructures create when jamming signals are directed at a vessel.

The trials undertook to test the ability of the GAS-1 and ADAP systems to cope with that aspect of jamming signal exposure.

The results of these shipboard exercises will help determine the best location for anti-jam systems on vessels.

Emissions countermeasures for ADF assets

High-value ADF assets to be offered protection using CRPA systems include the F/A-18 and AP-3C aircraft, Black Hawk and Seahawk helicopters, the Adelaide Class Guided Missile Frigates and Anzac Class Frigates.

The work on CRPA overall is part of a larger research effort being undertaken in this area under the Navigation Warfare Memorandum of Understanding that has been drawn up between the USA, UK, Australia and Canada.

In a further development related to this work, Tenix (now BAE Systems), working with the University of Adelaide, was recently awarded a contract in the current round of DSTO's Capability and Technology Demonstrator program to miniaturise the CRPA technology for application on platforms that have size, weight and power constraints, such as unmanned aerial vehicles.

Problem solving on the battle field

Australian Defence Force (ADF) commanders carrying out missions overseas have been increasingly calling on the services of deployed DSTO analysts to find solutions for operational problems, with great success.

Operations analysis (OA) can be described as the application of scientific methods to provide decision makers with a quantitative basis for making better decisions.

The concept of OA originated in the techniques of operations research developed in Britain in the early stages of World War II. It significantly benefited the British war effort by optimising the deployment of weapons systems and of military forces.

The application of OA within Australian military circles began during the latter stages of World War II, being first used in support of RAAF missions.

This technique of investigation was, until recently, only applied retrospectively to find out what lessons could be learned after an operation. These days, however, the need to undertake analysis also before and during operations is increasingly seen to be crucial.

The reasons for this are that the learning cycles of today's enemies are getting shorter, ever arriving at newly adaptive and unpredictable threats, which enable small, poorly equipped outfits to wield disproportionately high levels of impact. The upshot for ADF commanders is that they need to devise responses more flexibly and more quickly than before.

"The role of analysts is to provide on-site advice to commanders from a clear scientific viewpoint," explains LTCOL Jack Gregg, one of the managers of DSTO's deployed OA program. "Effectively, they are a resource that the commander carries in his or her back pocket, ready whenever needed."

"We provide analysis at the tactical level in support of commanders, in keeping with the relatively small scale of ADF operations and an emphasis on Force Protection. In US and UK Defence circles, by comparison, OA is only used at the highest strategic and operational levels."

The scientific methods used in OA

The OA problem-solving processes that analysts apply include two basic kinds, quantitative and qualitative, with both often being brought to bear when breaking down a problem.

A quantitative approach involves collecting data and undertaking 'number crunching' statistical or mathematical analysis that typically arrives at an optimal maximum or minimum figure for operational matters such as logistics support and force deployment.

One or more analytical tools may be applied from a range that includes optimisation, linear programming, probability theory, queuing theory, game theory, graph theory, decision analysis, simulations and reasoning. Some of the software applications analysts use are custom-written, while others, like Microsoft Excel, are commercially available.

A qualitative analytical approach involves collecting information about attitudes, opinions and beliefs via interviews, surveys and questionnaires in order to learn what a group of people in an operational zone think about an issue. This data is used by commanders to best formulate ways of working with coalition partners and friendly locals or overcoming an enemy.

For example, a deployed commander wanting to get a message of some kind out to local nationals could request a study be carried out. The study would establish the most effective and credible means of communicating, taking into consideration factors such as the available media forms and how best to craft the message.

While OA firstly developed as a quantitative process, analysts are increasingly required to know about, and apply, qualitative appraisals now that commanders have been placing greater reliance on this form of inquiry.

"This shift in emphasis over the last five years reflects a growing awareness that the only way to attain mission success in many cases is through appreciation of the human environment," says LTCOL Gregg.

Main photo and opposite page: scenes of life taken by DSTO Operations Analysts on deployment.

Applying OA techniques in the field

Deployed OA work is sometimes done on an individual basis, but is more commonly carried out in pairs involving a military member and a civilian scientist. Occasionally, syndicates of four to five, involving a mix of these two personnel types, may combine to work on a problem.

To begin the OA process, the commander sets the scene for a task or mission, and outlines the courses of action open to him or her. This description includes discussion about how the task is to be accomplished together with use of OA resources in support.

The deployed OA personnel then undertake to correctly articulate the problem, involving a round of iterations with the commander to ensure they have 'got it right'. They next devise a plan to carry out their OA work, which generally involves collecting data, conducting analysis, and presenting their findings.

Before starting work, the commander reviews the OA plan to confirm that the problem has been correctly identified. After the plan is approved, the commander arranges to make available any resources or permissions required that the analysts may need to carry out the OA task, and then the analysis plan is put into action.

The solutions arrived at through analysis are delivered back to commanders within periods of two to three weeks, sometimes even overnight in cases where extreme urgency is required.

The ADF's deployed analysts are supported by a 'reachback' facility that enables them to call on the services of DSTO researchers within Australia to assist with problems they are unable to solve alone.

Via a video link support service, deployed analysts can discuss issues and problems directly with researchers back in DSTO as well as with other analysts connected by the same video link. Often, the deployed analysts find that many problems they face are similar, and that these sessions lead to problem solving through cross-pollination of ideas.

DSTO's deployed OA program

DSTO is responsible for selecting, training and assigning deployments for both the civilian and military components of OA teams. This is undertaken through an intensive four-week live-in training activity called the Joint Pre-deployment Operations Analysis Course (JPOAC). The most recent course was presented at HMAS Harman in the ACT.

After having run JPOAC now for three years, DSTO is able to provide a minimum of seven analysts for deployment at any one time, with a further seven available on a 'surge' basis if required to cover a particular problem. Analysts are currently deployed in support of joint missions in Afghanistan, Iraq, East Timor, and the Northern Arabian Gulf (NAG).

Recent examples of OA work carried out by DSTO include analysis of improvised explosive device placements and insurgent activities, a review of the use of air transport for personnel and logistics movements, a study of HQ responses to emergency situations, and protection of oil platforms in the Northern Arabian Gulf.

According to Dr Nanda Nandagopal, DSTO's Deputy Chief Defence Scientist (Policy and Programs), the role of deployed operational analysts is critical for a quick understanding and response to emerging threats. "They are making a huge difference to ADF efforts to combat opponents such as the Taliban in Afghanistan," he says. " Without these contributions, our commanders would be really stretched."

The value of deployed OA personnel in support of commanders in the field has been recognised by the ADF to the point that several high-ranking officers, including MAJGEN Mark Evans, LTGEN David Hurley (Vice Chief of the Defence Force) and LTGEN Ken Gillespie (Chief of Army), have given it their enthusiastic endorsement.

Communications security in the palm of your hand

A prototype communications device that deals simultaneously with classified information at different levels has been developed by DSTO to overcome security issues stifling information flows between coalition partners in today's network centric warfare environment.

The need for a device like MiniSec2, explains DSTO researcher Dr Duncan Grove, arises because information flows within a military environment take place at different security levels, which must be strictly partitioned.

"Traditionally, the way of dealing with this requirement has been to duplicate computing and network resources in isolation for each security level, resulting in extensive and costly system replication.

"The MiniSec2 hand-held device custom-built by DSTO overcomes this problem in one small package, providing Multi-Level Secure (MLS) pervasive mobile voice and data communications.

"However, while MiniSec2 is currently capable of simultaneously processing information at different security levels from unclassified to top secret, it is yet to be accredited for such use by the relevant security organisations."

MiniSec2 in a nutshell

MiniSec2 incorporates four self-contained central processing units (CPUs), hardware encryption facilities, trusted display and audio input-output (I/O), and multi-modal wireless capabilities.

It has four buttons on the side of its case, each corresponding to one of the device's four CPUs.

When one of these buttons is pressed, the designated CPU is securely and exclusively connected to the device's touch screen and audio interfaces. Meanwhile, the other CPUs, and the applications running on them, continue to function in the background, able to be recalled at the press of a button.

One resource that all CPUs maintain continual access to, however, is the network. Although all CPUs use the same underlying physical network – for example WiFi, fixed Ethernet, 3G or satcom – traffic to and from each CPU is kept cryptographically separated, resulting in what is known as a partitioned communication system.

These strict isolation mechanisms allow the different CPUs to securely process information at different security levels.

A wearable speakerphone accessory for MiniSec2

Audio I/O functionality for the MiniSec2 is provided via a device named Button that clips on to a wearer's shirt collar.

Individually paired with a particular MiniSec2, this device facilitates secure point-to-point or conference calls, or unclassified interconnection to civilian telephone networks.

Button is based on Bluetooth audio technology, but its security has been enhanced to levels beyond that offered by commercially available systems.

This has been achieved by including dedicated hardware-based encryption with provision for secure physical keying, in addition to a tri-colour Light Emitting Diode indicator that shows the security status of the microphone.

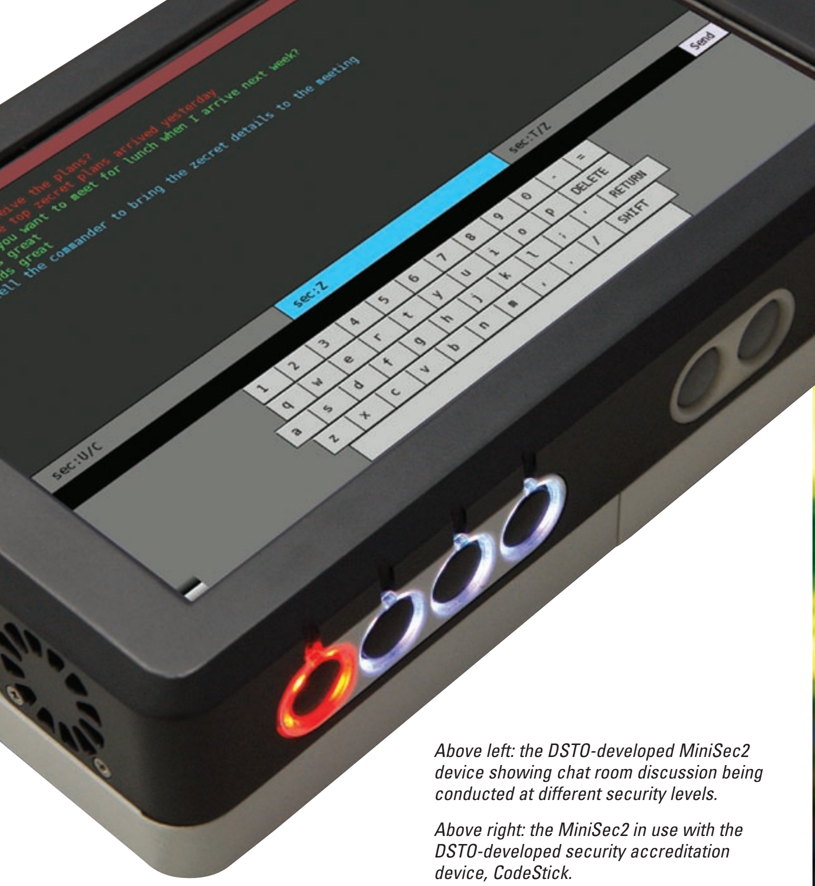
'Multiple' versus 'Multiple Independent' Levels of Security

Three of the MiniSec2's four CPUs are used to support Multiple Independent Levels of Security (MILS) operating modes, at 'unclassified', 'secret', and 'top secret' levels.

The advantage of these modes is that they can run unmodified, commercially available operating systems and software – including web browsers, email applications, Voice Over Internet Protocol (VOIP) clients, and more – safely and securely within classification-isolated partitions.

A disadvantage, however, is that strict partitioning forces the user to keep switching between modes when they need to access information at different security levels.

Meanwhile, the fourth CPU runs a proprietary operating system and application environment developed by DSTO, called Annex, which can securely process information at different security levels all on the same CPU.


Send
sec:T/Z
sec:Z
sec:U/C
ve the plans?
top secret plans arrived yesterday
you want to meet for lunch when I arrive next week?
ds great
all the commander to bring the zecret details to the meeting
DELETE
RETURN
SHIFT

Above left: the DSTO-developed MiniSec2 device showing chat room discussion being conducted at different security levels.

Above right: the MiniSec2 in use with the DSTO-developed security accreditation device, CodeStick.

This allows what are known as Multi Level Secure (MLS) applications to be developed for use on the MiniSec2 that can provide rich, interactive access to information at many different security levels, all from within the same application.

One such example is the Annex Instant Messenger application, which enables users to enter virtual chat rooms where they can send and receive differently classified messages, but only up to the level of their security clearance.

Other MLS applications being developed include Blue Force tracking of deployed forces during operations, network management, and document editing systems.

Secure mobile communications using commercial networks

The MiniSec2 and Button devices are seen to have uses for a number of secure communications activities, particularly telephony and video conferencing.

The security measures built into the MiniSec2 system also make it possible to conduct secure communications at various security levels, separately or simultaneously, over a single unclassified third-party communication network.

MiniSec2 devices also have the ability to roam using Mobile IP on any IPv6 network (the next-generation Internet Protocol standard) including the internet itself, and existing network sessions and applications will continue to function without any user intervention.

To ensure compatibility with other devices and systems that use the current IPv4 standard, the MiniSec2 can also interoperate with IPv4 networks via legacy tunneling mechanisms.

The Annex suite of secure communications devices

The MiniSec2 device belongs to a suite of prototype hand-held or wearable devices being developed by DSTO. These are collectively known as the Annex ensemble. Other devices in the ensemble include Button and CodeStick.

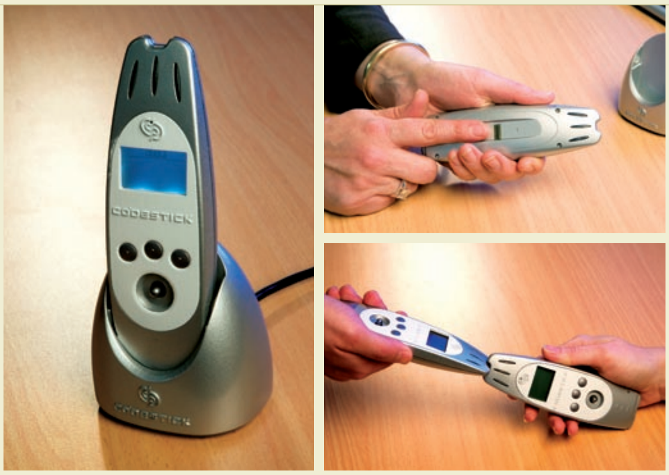
Each device is provided with a unique identity at the time of manufacture, distinguishing it from any other within the Annex network.

All Annex components are personalised for the particular individual to whom they are issued, carrying a collection of secure non-forgeable, authority-carrying references called ‘capabilities’ which allow them to perform security-controlled actions on their owner’s behalf.

The purpose of the Annex ensemble is to provide secure enhanced connectivity between different coalition forces as well as seamless connectivity to civilian entities, using standard Internet Protocols.

The Annex security architecture has been designed to support the principles of least authority, mutual suspicion and need to know, thereby allowing autonomous, mutually suspicious organisations to operate in coalition.

CodeStick:
on-the-spot security check


The DSTO-developed CodeStick device.

DSTO has developed a prototype security device that personnel can use to rapidly confirm each other's identity and security clearances upon meeting, and also to access secure facilities and computer networks.

CodeStick forms part of an ensemble, known as Annex, being developed by DSTO to facilitate multi level secure pervasive mobile voice and data communications. Other devices in this ensemble include MiniSec2 and Button.

"A novel function of CodeStick," explains DSTO researcher Dr Damian Marriott, "is to provide peer-to-peer trusted and strong authentication for checking of security credentials without recourse to third parties or infrastructure, thus eliminating the need to forward on security clearance details in advance of meetings.

"This device also eliminates the need for Defence personnel to remember multiple passwords, or carry around multiple security tokens."

Each CodeStick device is readied for use with a biometric authentication process. Since an individual unit therefore can only be used by the person it was issued to, the technology is designed to provide very high levels of security assurance.

A portable package of security data and passwords

The CodeStick device, about the size and shape of a small household remote-control unit, fits in the hand when in use, and can be readily carried in a pocket or briefcase at other times.

CodeStick devices can communicate with one another and other kinds of electronic equipment, such as computers and secure door swipe pads, via short-range directed radio links.

The limited scope of communications together with secure cryptographic protocols ensures that only the intended recipient device can receive and decode data being sent.

Security features designed into the device include biometric authentication, Elliptic Curve Cryptography authentication process, Advanced Encryption Standard encrypted communications, two factor secure logon, e-mail encryption and signatures, secure storage of credentials for web-based logon, and a formally modelled design for high assurance evaluation.

Secure face-to-face credential checking

Two personnel wanting to exchange personal security credentials can do so quickly and directly with their own personalised CodeSticks.

Users simply position the devices close to each other, enter a query and press a button. Information about the security authorisation level of each person is immediately received, decoded and the highest authorisation level common to each person in the query is displayed on the read-out panel of the other person's device.

A notable feature of the process is that it does not unnecessarily expose the highest security details of the participants to each other.

The CodeStick technology offers a substantial improvement on Defence's current credential exchange system, in which each person must get their own security officer to manually exchange clearance information with the other's security officer – an awkward, slow and error-prone process.

Other security access functions

CodeStick also eliminates the need for passwords to access Defence networks, having a single sign-on capability that enables secure logon to PCs and web-based systems. It supports secure messaging by encrypting and digitally signing email messages.

Additionally, CodeStick provides a means of gaining physical access to secure areas. To open a secure door, the device is simply held close to the secure access swipe panel, in similar manner to the current process of swiping a card over the panel to gain access.

Many functions of CodeStick have already reached stable operation, and a user trial of the device is now being prepared.

Uses envisaged for the technology include a range activities such as securely enabling weapons systems, tactical Blue Force tracking of deployed forces during operations, access control for classified meetings and conferences, interaction with other devices in the Annex ensemble, and various ultra high assurance functions.

DSTO and Raytheon to work on intelligence system

DSTO recently signed a cooperative research and development agreement with Raytheon Australia for a project involving a web-based system that enables intelligence sharing among warfighters in near real-time conditions.

The Distributed Common Ground System (DCGS) and DCGS Integration Backbone applications, developed by Raytheon for US Defence, were devised for the purpose of facilitating distribution of the right information at the right time to maximise operational effectiveness.

The collaborative venture will undertake to demonstrate, test and evaluate the performance of Raytheon's product in an Australian intelligence, surveillance and reconnaissance context.

DSTO has established a laboratory at its Edinburgh site where the two partners will work together to incorporate software applications into the system in preparation for its use by the Australian Defence Force (ADF).

The project is expected to further understandings generally of the utility of such systems for ADF applications.

Ron Fisher, Managing Director of Raytheon Australia (left), and Dr Ian Sare, Acting Chief Defence Scientist, at the signing of the DSTO-Raytheon agreement.

Air guns for underwater shock testing

DSTO has been conducting research on the use of seismic air guns as an alternative to the detonation of explosive charges for shock testing the equipment fit and structural integrity of naval vessels.

The main advantage offered by air guns is that they produce a relatively low-level energy output compared to that of explosives.

They can thus be used in relatively shallow water, such as an inlet or river system, without unduly disturbing the environs. This means the process of setting up a trial need not involve locating to a more remote blue water site.

Although the relative amount of energy given out by a single air gun is not large, when used in arrays of as many as 20 guns, they can jointly generate localised shock loadings on a vessel large enough for study purposes.

A full-pressure trial of two seismic air guns was recently carried out at DSTO's Melbourne Underwater Test Facility.

The trial was attended by US research personnel, who are undertaking studies of the technology for the US Navy. These US researchers have expressed interest in collaborating with DSTO on this work.

Analysing aircraft wear debris made easy

DSTO has commissioned a metallic wear-debris analysis capability in the Navy Aviation Systems Program Office (NASPO) at HMAS Albatross, Nowra, NSW.

The analysis is conducted using an X-ray fluorescence machine that enables the elemental composition of metallic wear debris retrieved from aircraft magnetic chip detectors and oil filters to be determined.

Training for use of the equipment was provided to NASPO staff by DSTO.

Prior to this, analysis procedures involved the work of DSTO staff using scanning electron microscopes for an inspection process that was generally routine and not requiring high-level scientific expertise, and the turnaround time for delivery of results was several days.

NASPO is now able to carry out the analysis on-site, thereby allowing same-day analysis of the majority of wear debris. This capability provides valuable information about aircraft machinery health, which can confirm the need for removal of engines or gearboxes and help prevent premature removal.

The new capability also frees up DSTO scientists to apply their expertise to new or non-routine problems.

DSTO's minesweeping system for Indian Navy

The Australian Minesweeping System, developed by DSTO, was recently exported to India in what is the largest ever overseas order for this innovative technology.

Thales Australia, which markets the technology, recently presented DSTO with a royalty cheque of $514,358 for the export sale to India.

The Australian Minesweeping System is now in service with the navies of nine countries.

To date, the system has earned $78 million in export sales.

CALENDAR

28 Sept–1 Oct 2008	The Third International Conference on Bio-Inspired Computing National Wine Centre of Australia, Adelaide South Australia **www.bic-ta.org**
29 Sept–1 Oct 2008	Nanotechnology and Applications Crete, Greece **www.iasted.org/CONFERENCES/home-615.html**
14–15 Oct 2008	Defence Human Sciences Symposium DSTO Edinburgh, Edinburgh South Australia **www.dsto.defence.gov.au/events/dhss**
27–31 Oct 2008	Land Warfare Conference 2008 Brisbane Convention and Exhibition Centre Brisbane **www.dsto.defence.gov.au/events/lwc2008**
16–18 Nov 2008	Parallel and Distributed Computing and Systems Orlando, Florida, USA **www.iasted.org/CONFERENCES/home-631.html**
16–18 Nov 2008	Environmental Modelling and Simulation Orlando, Florida, USA **www.iasted.org/CONFERENCES/home-638.html**
17–19 Feb 2009	Artificial Intelligence and Applications Innsbruck, Austria **www.iasted.org/CONFERENCES/home-639.htm**
17–19 Feb 2009	Signal Processing, Pattern Recognition and Applications Innsbruck, Austria **www.iasted.org/CONFERENCES/home-643.html**
23–26 Mar 2009	Health and Usage Monitoring Systems 2009 DSTO Fishermans Bend, Grand Hyatt Melbourne, Avalon Airport Victoria **www.dsto.defence.gov.au/HUMS2009**

ADS16/1 2008 8347 *Cover image: CBR clothing being tested on articulated mannequin.*