

# PRIME MINISTER'S SCIENCE, ENGINEERING AND INNOVATION COUNCIL

**NINTH MEETING – 5 December 2002**

## **AGENDA ITEM 3**

---

---

### **SCIENCE AND SECURITY**

#### **Executive Summary**

The face of terrorism has been changing, as was brought home to Australia and the working group with the tragic events in Bali. Australia's counter-terrorism strategies and activities must keep pace with this changing threat. Contemporary terrorism is more likely to involve the impact of coordinated, large explosives and/or chemical, biological or radiological events as well as cyber threats. Our science, engineering and technology (SET) base can, and must, contribute to all phases involved in combating terrorism including detection, prevention, response and recovery. Strong SET support will be a major factor in keeping us ahead of the threat rather than just reacting to events as they occur.

Although the working group's title of Science and Security implies a broad range of events, both deliberate and accidental, the group's remit was to focus on strengthening the links between Australia's SET and current and future counter-terrorism needs. Recommendations of the group may still have application to the broader topic of security.

The working group found that Australia's SET community does not have a focus for our counter-terrorism needs. Therefore, this report suggests a framework to enhance collaboration between the SET community and the operational side of counter-terrorism. The framework provides mechanisms to leverage existing R&D as well as encourage more focused research to support national security. Within this framework the working group recommends:

1. A SET unit to be formed with additional SET funding as the first point of contact for harnessing SET for counter-terrorism in Australia. The new unit would bring

together national and state counter-terrorism SET requirements, resources, interests and agencies.

2. The proposed unit would focus on SET support for developing counter-terrorism capabilities and analysis of critical infrastructure vulnerabilities.
3. The new SET unit will be the primary focus for international collaboration in SET counter-terrorism.
4. The unit will develop a portfolio management process for SET support for counter-terrorism via developing and maintaining a SET inventory for potential support of counter-terrorism; promoting SET requirements and gaps; and establishing collaborative programmes and activities and recognition mechanisms.
5. National security to be included as a national research priority.

In coming to its recommendations, the working group used a two-step process to assess Australia's SET base to support counter terrorism, at all times operating in an unclassified environment. Firstly, the group identified priority research areas after hearing from a range of experts. Secondly, the group conducted a preliminary survey of the Australian SET base against these priorities.

The working group came into contact with a range of experts who provided the context for their deliberations. This context went well past the strict Terms of Reference for the group to include such things as our state of readiness.

The tragedy in Bali has alerted the Australian public to the threat of terrorism. It is the hope of the working group that this new awareness will lead to a better prepared Australia and the saving of a multitude of lives in the future.

## Contents

Executive Summary .....	i
Contents .....	iii
Introduction and overview .....	1
International activities .....	3
Australia's preparedness to deal with terrorism .....	5
Working group's methodology .....	6
Recommendations and path forward .....	9
Glossary .....	14
Appendix 1: Terms of Reference.....	16
Appendix 2: Membership of the PMSEIC Working Group on Science and Security.....	17
Appendix 3: List of presenters to the working group .....	18
Appendix 4: SET survey e-mailed to private and public researchers.....	19
Appendix 5: Recommendations on SET support for biological threats .....	22
Appendix 6: Case studies.....	24

# Introduction and overview

## Introduction

The events of 11 September 2001 heralded a shift in global conventional wisdom concerning the nature and spectrum of terrorism threats. These changes include an appreciation that less frequent but larger scale terrorist events, the employment of aircraft and large bombs, potential use of chemical, biological and radiological (CBR) agents and computer network operations are emerging as contemporary terrorist tactics. Similarly, the aim of terrorism is recognised as having evolved beyond being a coercive political tool, to include the objectives of terrorising entire populations and a mechanism for attacking a nation state. Further, the symbiotic relationship between terrorism and the pervasive impact of global media reporting are recognised as a principal factor in the application of terrorism as a powerful asymmetric threat option. Predominant in this equation are the scale and impact of physical and psychological effects on the Australian public.

Within this context the 2002 Australian Leaders' Summit directed that contemporary counter-terrorism (CT) capabilities be developed to counter the new risk to Australian interests. Governments' commitment to this effort is reflected in the substantial resourcing of the Commonwealth security agencies in the wake of the recent Bali incident and threats to critical infrastructure. Inherent in this guidance is the requirement to develop national counter-terrorism capabilities at a level of sophistication that can only be supported by Australia's very best science and technology and access to world's best SET through international collaborations.

Defence against the asymmetric threat terrorism poses requires a national effort across a broad front of government (federal/state/territory), national bodies, the armed forces, industry and the science community. Science, engineering and technology (SET) can contribute to all phases involved in combating terrorism, namely, intelligence and surveillance, prevention, protection, interdiction, response and recovery, and attribution. Australia's SET can position us to meet current threats and, with a longer term view, provide novel solutions for future threats. SET provides the foundation to staying ahead of the threat.

However, the existing environment for SET support to counter-terrorism is uncoordinated and inefficient in national terms. There are a large number of government and private sector organisations with the potential to contribute both as clients and as providers. There are also a variety of formal and informal domestic and international linkages in place.

**It is therefore timely to establish a framework for future collaboration in science, engineering and technology that provides direction to policy makers on mechanisms for developing appropriate measures to counter those threats.**

The working group recognised that while its title of 'Science and Security' suggests a broader remit than counter terrorism activities, the Terms of Reference (see Appendix 1) required the group to focus on strengthening the links between Australia's SET and current and future counter-terrorism needs. The working group suggests that its recommendations may have application to the broader topic of security.

## The challenges of contemporary terrorism

Contemporary terrorism is considerably different to the threats on which Australia's counter-terrorism architectures and capabilities were first established. In developing contemporary counter measures to terrorism, Australia now faces an unprecedented range of threats and scale of impacts. Our modern counter-terrorism measures must now focus on preventing actions by sophisticated and potentially undeterrable terrorists, responding to widespread, complex, coordinated attacks and recovering from near catastrophic events. Contemporary counter-terrorism must therefore focus on preventing terrorist actions. This requires a national level response, beyond the capacity of one State or Territory to cope with. Such events are

likely to involve attacks on infrastructure and the employment of heavy casualty weapons including very large bombs and CBR agents.

### **The case for Government action**

There is no existing program for SET support to Australia's counter-terrorism capabilities. This has been and remains a critical shortfall in the national capacity to deal with terrorism. Moreover, the nature of emergent global terrorism is such that there are clear imperatives for such a program as evidenced by activities of the following bodies:

*Technical Support Working Group (TSWG).* Australia has been approached by the TSWG, a US inter-agency group overseen by the Department of State, to be involved in a bilateral relationship. The TSWG was created for the purpose of coordinating and funding SET that could directly support counter-terrorism outcomes. Currently TSWG has bilateral arrangements with the UK, Canada and Israel, and it is likely Australia will be the only other nation invited to participate. The partnership would involve shared funding activities and opportunities for Australian agencies and industry participants to expand their customer base. One of the drivers behind the formation of this PMSEIC working group was to undertake the work necessary to allow Australia to make an informed response to the approach by the TSWG. The US has made it clear that participation requires the existence of a central coordinating agency, a single national point of contact, and identification of funding. ***A number of possible joint projects have already been identified which can only be implemented following the formation of the coordinating body.***

*National Counter Terrorism Committee (NCTC).* The NCTC does not have a SET program integral to its capability development process, instead relying on indirect benefit from State and Commonwealth research projects, most notably those of the Defence Science and Technology Organisation (DSTO). The recommendations in this report address this issue.

*Critical Infrastructure Advisory Council (CIAC).* Recent Cabinet submissions have recommended the formation of the CIAC to oversee critical infrastructure (CI) protection and development. Their recommendations include establishing a Cooperative Research Centre (CRC) for Infrastructure Protection. DSTO has independently recognised the merit of considering the role, nature and tasks of a Centre for Analysis of Critical Infrastructure. The impetus to the CIAC proposal given by integrating these initiatives is compelling and could be advanced under a focussed SET program. ***There is no doubt that a CRC could facilitate the research aspect of these issues but CIAC would need to also address the collaboration and coordination function which led the working group to Recommendation 1.***

*Defence Science and Technology Organisation.* DSTO's role in supporting defence related counter-terrorism capability development is complementary to the wider national requirements. Initial discussions suggest there is a high degree of commonality in research requirements and considerable benefit to Australian scientific endeavour, if DSTO counter-terrorism related research can be better coordinated with Australia's wider efforts.

*Industry / Public portal.* There is no clear line of access between Government interests in counter-terrorism development and the initiatives and entrepreneurial skills of Australian industry. Both the USA and Canada have developed mechanisms to manage a secure interface between national security interests in SET and industry. ***However, in Australia there is no clear architecture to advise existing industry support groups such as the Australian Industry Defence Network, on priorities specifically for SET counter-terrorism requirements.*** This is clearly a limiting factor in Australia's potential for leveraging off excellent science and promoting innovative Australia industries. Similarly, there are a substantial number of independent and collaborative academic programs currently relevant to counter-terrorism. These are being limited in their potential by a lack of integration into a wider national program focussed on SET support to counter-terrorism efforts.

## International activities

Australia is not the only country looking at how to better access its SET base to ensure that development of counter-terrorism applications takes into account the best R&D projects whose primary focus may not be counter-terrorism. Given the limited resources and time available to the working group, we did not carry out an exhaustive international evaluation of SET support for counter-terrorism activities.

The US and Canadian situations, examined in more detail below, were chosen because of an approach on the part of the US to interact with Australia in this arena, and because of strong similarities between the Australian and Canadian federal systems. Both Canada and the US also maintain defence science organisations similar to Australia's DSTO, such as the US Defense Advanced Research Projects Agency.

Australia's interaction with Asia Pacific nations on security matters is largely achieved through the ASEAN Regional Forum and some bilateral agreements (refer to [www.dfat.gov.au/arf/pub98bil.html](http://www.dfat.gov.au/arf/pub98bil.html)) and participation in the multilateral ASEAN Regional Forum. With the heightened threat to Australian interests in the region, productive counter-terrorism networks are constantly being created, developed and enhanced. Many such networks, however, remain in their infancy. SET support to any such networks is similarly under-developed, so **Australia has the opportunity to take a leading role in SET support to counter-terrorism in the Asia-Pacific region.**

## United States of America

The Department of State, in the USA, through the Office of the Coordinator for Counterterrorism, has primary responsibility for developing, coordinating, and implementing American counterterrorism policy. The US Technical Support Working Group (TSWG), as mentioned above, was established in 1982 as a subgroup of the then Interdepartmental Working Group on Terrorism under the US Department of State. The TSWG mandate is to develop counter-terrorism technology as a stand-alone interagency working group. In recognition of the existing and growing interdependence of critical infrastructure, a centre has been established to improve the understanding of America's critical infrastructure system. The Centre will report to the Critical Infrastructure Protection and Continuity Board on which the Department of State is represented.

### *US Technical Support Working Group*

The TSWG is the national forum that identifies, prioritises, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community. It addresses joint international operational requirements through cooperative R&D with the United Kingdom, Canada and Israel under separate bilateral agreements.

Participation is open to federal departments and agencies with funding derived principally from the Department of Defence's Combating Terrorism Technology Support Program. The Department of State and other Departments and agencies contribute additional funds, and personnel to act as project managers and technical advisors. Membership includes representatives from nearly 80 organisations across the Federal Government.

Departments and agencies work together by participating in one or more subgroups. The nine subgroups are: CBRN countermeasures; Explosives detection; Improvised device defeat; Infrastructure protection; Investigative support and forensics; Personnel protection; Physical security; Surveillance, collection and operations; and Tactical operations support.

### *US National Infrastructure Simulation and Analysis Center*

The US National Infrastructure Simulation and Analysis Center (NISAC) has been established as the first comprehensive capability to assess the system of infrastructures and their interdependencies. It provides services to the Critical Infrastructure Protection and Continuity Board. The Board's responsibilities are anticipated to include recommending policies and coordinating programs on critical infrastructure protection, information systems security, emergency preparedness communications, continuity of operations, and continuity of government.

NISAC will provide modelling, simulation, and analysis of the nation's infrastructures, with emphasis on interdependencies. This analysis will lead to optimized mitigation strategies and reconstruction planning and real time crisis support. NISAC will use distributed information systems architectures to provide virtual analysis capabilities that will accommodate a large number of providers and a large number of users. Its core partners are Sandia National Laboratories and Los Alamos National Laboratory.

### **Canada**

In Canada, as in Australia, the Department of the Solicitor General has the lead role in the planning, coordination and implementation of the Government's national security policies including Canada's counter-terrorism framework. In fulfilling its role, the Department works closely with other federal departments and agencies, provincial and territorial governments and the international community. R&D is fostered under a number of organisations including the Chemical Biological, Radiological and Nuclear Research & Technology Initiative (CRTI).

#### *Chemical, Biological, Radiological and Nuclear Research & Technology Initiative*

CRTI was launched in April 2002 as an interdepartmental initiative involving a number of agencies including the Office of Critical Infrastructure Protection and Emergency Preparedness, and the Solicitor General Canada. Defence R&D Canada leads the Initiative.

CRTI is mandated to strengthen Canada's preparedness for, prevention of and response to a CBRN attack by fostering new investments in research and technology through: the creation of clusters of federal laboratories; funding to build capability in critical areas; accelerating the delivery of technology to the first responders' community; and funding those areas in which national science and technology capacity is deficient owing to obsolete equipment, dated facilities or inadequate scientific teams.

Through CRTI, clusters of federal science laboratories work together to take a coordinated approach to CBRN emergencies. Through the project structure, they will partner with private-sector organizations and academic laboratories to increase the national science and technology capability to respond to CBRN threats.

#### *The Office of Critical Infrastructure Protection and Emergency Preparedness*

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIEPEP) was formed in February 2001 from the old Emergency Preparedness Canada organisation (equivalent to Emergency Management Australia) with an expanded role to include not just emergency management, but also cyber and physical infrastructure protection. It is a civilian organization operating within the Department of National Defence, and has a directorate of R&D to support its goals.

The directorate consists of a small number of staff, and undertakes its role via partnering with other agencies with the capability to undertake studies and research. Partnerships include other government departments, other levels of government, private sector, academia, non-governmental agencies and allies. The partnering is undertaken by several means:

- build on current capabilities and focus current work
- utilise grants and contributions from research councils

- a fellowship programme
- current funding of approx C\$2M pa for additional requirements.

In addition to the subject matter experts within OCIPEP dealing with the partnering arrangements, they also engage in internal analyses, and are extending a natural hazards computer model to allow interpretation for man-made vulnerabilities. This model has parallels with the Australian 'Cities' project.

OCIPEP also enhances the awareness and capacity of Canadians and their communities, businesses and governments to manage risks to their physical and cyber environments through a number of programs and various information products.

With the system of responsibilities for both critical infrastructure and the research capability to support it distributed between Provincial and Federal agencies, there are many parallels with the Australian situation and Australia could learn much from the Canadian experience. The working group suggests that Australia approach Canada to develop closer ties in this area.

## **Australia's preparedness to deal with terrorism**

Australia's counter-terrorism capabilities have been developing since their establishment in 1978. The security imperatives of the 2000 Olympic Games resulted in considerable development of several Commonwealth capabilities within the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and the Australian Defence Force (ADF). Commonwealth capabilities were further enhanced in response to 11 September 2001 and again under the Government's recently announced initiatives stemming from the Bali bombing. The capabilities of the south-eastern states benefited from the Olympics experience and the remaining jurisdictions have maintained their counter-terrorism capabilities in accordance with the Standing Advisory Committee on Commonwealth/State Cooperation on Protection against Violence (SAC-PAV)/National Counter Terrorism Committee program.

For a number of years, the Commonwealth's priority for counter-terrorism capability development has been clearly focussed on Commonwealth agencies. Under the Australian National Anti-terrorism Plan, the States are responsible to respond in the first instance, with the Commonwealth agencies providing support as needed. This accords with the standard policing and emergency services response to any incident.

The National Counter-Terrorism Committee (NCTC) was formed on 24 October 2002, when the Premiers, Chief Ministers and the Prime Minister signed the Inter-Governmental Agreement on counter-terrorism arrangements and flows from the decisions made by the Leaders' Summit on Transnational Crime and Terrorism in April 2002. It replaced SAC-PAV.

NCTC reports annually to the Council of Australian Governments on Australia's preparedness to deal with terrorism and its consequences. The first report, commissioned by the Prime Minister, Premiers and Chief Ministers on 24 October, will be delivered at the COAG meeting on 6 December 2002.

SAC-PAV/NCTC has engaged or participated in a number of reviews of aspects of counter-terrorism capability. These reviews have given NCTC a comprehensive base on which to continue and augment SAC-PAV's work and form the basis of its report to COAG on Australia's preparedness to deal with terrorism.

The working group came into contact with a range of experts who provided the context for their deliberations. This context went well past the strict Terms of Reference for the group to include such things as our state of readiness.

## Working group's methodology

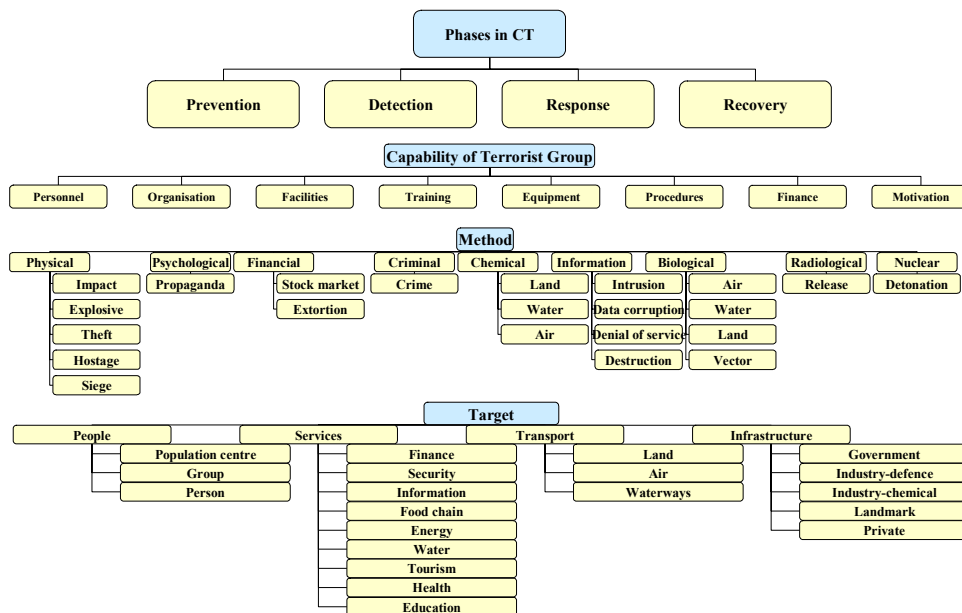
The working group used a two-step process to assess Australia's civilian SET base to support counter-terrorism. Firstly, the group identified priority research areas based on an assessment of risk. The group then conducted a preliminary survey of the Australian SET base against these priorities. ***At all times the group operated in an unclassified environment.***

### Identification of requirements for counter-terrorism research

Requirements for counter-terrorism research need to be based on the range of possible counter-terrorism threats and how Australia should deal with these threats.

The working group developed a matrix showing the phases in counter-terrorism, capabilities of terrorist groups, the methods that might be used in terrorist actions and the potential targets of such actions. This matrix, shown in Figure 1, demonstrates the breadth of the security problem. For each of these counter-terrorism threats, Australian action can be characterised by prevention, detection, response and recovery.

**Figure 1: Working group's matrix on counter-terrorism activities**



Speakers with expertise and responsibility in a number of areas in the matrix attended the working group and discussed current capabilities and gaps (see Appendix 3). Consideration of this information in the context of the overall problem led to the development of a priority list for counter-terrorism SET by the working group as listed below in order of priority:

1. population attack – response
2. explosive – prevention, detection, response
3. biological – prevention, detection, response\*
4. terrorist detection
5. community outreach
6. essential services – prevention, detection
7. chemical attack

8. cyber attack
9. air transport – prevention (regional)
10. infrastructure / landmark

\* A detailed analysis of the biological threat and recommendations on a way forward are described in Appendix 5.

### **Survey of Australia's SET base**

The working group considered that while there is no focused research program in Australia for counter-terrorism or security, there were potentially a number of current research activities that would have possible application. The working group attempted to assess the extent of these activities quickly via an e-mail survey of Australia's current SET base. The survey was conducted prior to the events in Bali.

The e-mail was distributed through mailing lists including the Fellowship of the Australian Academy of Science, membership of the Academy's 30 National Scientific Committees, Pro Vice Chancellors (Research), government funded research agencies, the Australian Technology Showcase, the Australian Industry Network, the Australian Business Limited and Australian Security Industry Association Limited. A copy of the survey is at Appendix 4.

The Australian Research Council (ARC), on behalf of the working group, carried out a key word search of its grant management database to identify the magnitude and extent of funded research in areas of potential application to national security and counter-terrorism. The search was conducted on all ARC grants and awards that commenced their funding in 1998 or subsequently. The NHMRC also carried out a key word search on grants with a budget during or since year 2000. As NHMRC grants are directed at health and medical research, the results have a limited application across the complete priority list for counter-terrorism SET identified by the working group in the previous section. The NHMRC data is expanded in Appendix 5.

Neither the working group's survey nor the data provided by the ARC or NHMRC should be interpreted as representing the totality of national security and counter-terrorism research. Rather, the information indicates research activity in areas of science and technology that may be applicable to these areas. Further, claims by respondents to the working group's survey on the value / applicability of their research have not been verified. The working group was simply testing the water to determine the relative scale of Australian SET projects for counter-terrorism and the degree of difficulty in developing a transparent inventory of quality projects.

### **Results of the e-mail survey**

There were approximately 130 bona fide responses to the survey<sup>1</sup>. Over 50 responses were received from government organisations with around 40 responses from each of academe and the private sector. In cases where projects are of a collaborative nature, the survey response was categorised against the location of the respondent. Data has been presented in this report in its collated form to ensure that commercial-in-confidence information is protected.

The table below sets out the results of the survey and the ARC search by broad subject matter areas.

---

<sup>1</sup> These are the responses received in the timeframe allowed for the survey. Responses that were received by the working group after this time, may not have been incorporated into the final analysis.

**Table 1: Australian R&D projects by subject**

Subject matter of research	Number of projects	
	Survey	ARC
E-security, cryptography, communications, identification	42	45
Robotics and autonomous vehicles	1	20
Structures, blasts, fire issues, inventory/detection, weapons	35	29
Toxins, pathogens, contamination, water treatment, air quality and dispersion	36	46
Other (including social and political behaviour)	18	8

The responses to the survey were then sorted against the working group's priority areas. Of the 130 valid responses to the survey, those that did not match the priorities from the SET coverage matrix were eliminated – leaving some 60 projects for priority review. Examination of the descriptions of these projects narrowed the focus to 38 projects. These were then sorted against the group's risk categories and priorities and all project descriptions were looked at to check no projects had been missed.

The survey did not highlight many research projects in the fields of robotics / autonomous vehicles. Given the low key nature of the survey, the reason for the lack of response in this area cannot be determined. It may be a result of the survey not reaching researchers / developers in these fields, or researchers are not aware of the applicability of their projects to counter-terrorism activities. The ARC data confirms that there is a substantial body of work in this area.

**Table 2: No of responses against priority areas**

Priority areas set by working group for SET support	Number of responses
Population attack – response (includes infrastructure, essential services)	5
Explosive – prevention, detection, response	9
Biological – prevention, detection, response	9
Terrorist detection	7
Community outreach	-
Essential services – prevention, detection (water, energy, communications), includes cyber attack	3
Chemical attack	5

The working group does not want to draw any firm conclusions on the status of Australia's R&D from the survey recognising its limitations.

Rather, members concluded that the response to ***the survey demonstrated the ease with which a more rigorous audit of Australia's SET base could be conducted.*** An audit of the SET base would be a first step in better understanding the depth of R&D in Australia and where Australia's expertise currently lies to enable improved communication and collaboration between the providers of counter-terrorism applications with the users.

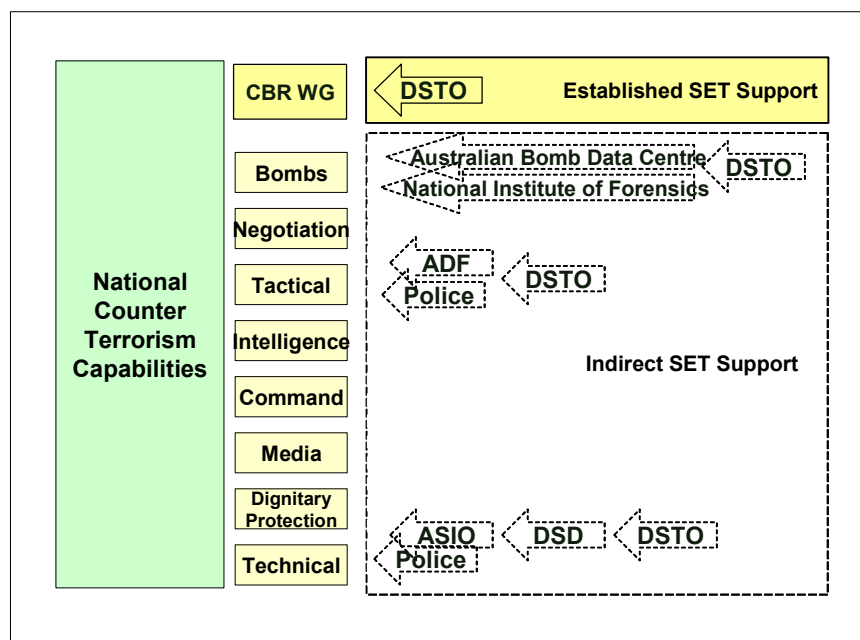
A second conclusion from the survey is that a more thorough audit of the SET base would require a targeted communications exercise to **encourage researchers to broaden their current parameters to how their research could be applied to counter-terrorism activities**. Some of the nil responses to the working group's survey were amended to more positive responses on prompting by members who understood the R&D being undertaken and its potential applicability to counter-terrorism activities. This result should not be surprising given that much of the university research was funded as 'discovery' grants which quite properly focus on the excellence of the science, rather than the immediacy of the applications. It is likely that events in Bali have since heightened awareness in the SET community of possible relevance of civilian research to support counter-terrorism activities.

The working group supports the audit process of research in Australia, being conducted by the four Academies: The Australian Academy of Science, the Australian Academy of Technological Sciences & Engineering, the Academy of the Social Sciences in Australia, and the Australian Academy of the Humanities. Involving the four Academies will ensure the highest possible capture and quality of Australia's R&D base. **In recognition that audits are current only for a short period, the working group suggests that each year one or two sections of the audit could be up-dated on a rotating basis (see recommendation 4).**

## Recommendations and path forward

The working group mapped out the accountability / responsibility for coordinating SET support for the prevention, detection, recovery and response phases of counter-terrorism activities as shown in Figure 2.

**Figure 2: National counter-terrorism SET support map**



It is the belief of the working group that the links between agencies and governments for SET support to combating terrorism in Australia are weak. A single co-ordinating unit would be the most appropriate mechanism to ensure greater collaboration between SET agencies while respecting the pluralistic framework of Australia's SET base. The working group strongly supports that such a unit be located as close as possible to operational accountability for counter-terrorism. The Attorney-General's Department (AG's) and the Department of the Prime Minister and Cabinet (PM&C) would be obvious candidates. Should the unit be placed in one of the major science agencies, e.g. DSTO, the linkages to AG's or PM&C would have to be very

clear. The unit would use partnerships and other collaborative mechanisms to coordinate studies and research utilising only a small number of staff.

#### Recommendation 1

A SET unit to be formed, with additional SET funding, as the first point of contact for harnessing SET for counter-terrorism in Australia. The new unit would bring together national and state counter-terrorism SET requirements, resources, interests and agencies.

### Preparedness, focus and strategy

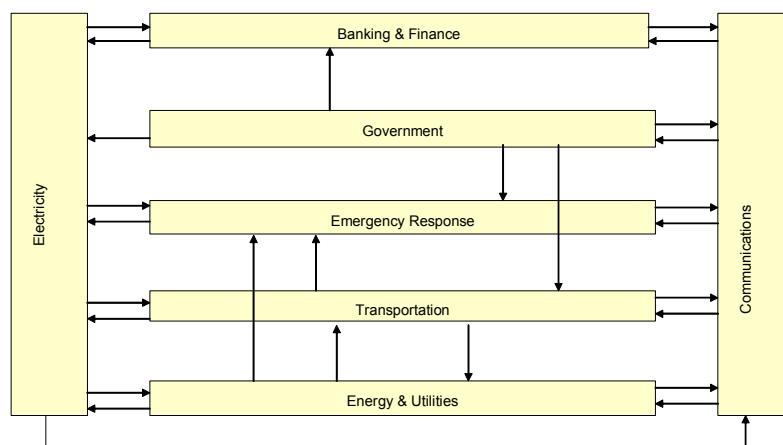
Preparedness, focus and strategy is about ensuring leadership on planning, connectivity and accelerating good science by exploiting existing National Counter Terrorism Committee arrangements.

The working group envisages the proposed SET unit incorporating existing national counter-terrorism priorities and having the following accountabilities:

- maps the SET support for counter-terrorism in close cooperation with CSIRO, DSTO and the four Academies;
- ensures duplication of effort is avoided; and
- SET activity is concentrated on national priorities for security.

In co-ordinating SET capability and improving collaboration, the proposed unit could use existing resources such as the National CBR Working Group under the Australian Emergency Management Committee, Geoscience Australia, DSTO, CSIRO, universities, cooperative research centres and industry-based research organisations.

**Figure 3: Critical infrastructure interdependencies simplified**



The proposed unit could also use pertinent industry groups to identify specific / critical infrastructure<sup>2</sup> vulnerabilities and establish prevention, mitigation and recovery strategies. The proposed unit would also be accountable for assessing the economic consequence of potential terrorist actions. Currently, a large number of government and private agencies are responsible for management and protection of critical infrastructure which are interdependent and involve

<sup>2</sup> Critical infrastructure comprises energy and utilities; transportation; communications; safety; financial, food and health services; and government services

complex interactions between systems (see Figure 3). **However, the working group believes there is no single group today focusing on analysis of critical infrastructure and therefore the working group recommends:**

#### Recommendation 2

The proposed unit would focus on two key areas

- SET support for developing counter-terrorism capabilities
- analysis of critical infrastructure vulnerabilities.

In summary, the working group believes it is essential that a single unit be responsible for:

- analysis and modelling of the potential impact of a terrorist event including supporting planning for development of critical infrastructure;
- identifying vulnerabilities and development of mitigations strategies;
- testing crisis management procedures;
- supporting training and education; and
- providing a forum for cooperation between agencies.

#### Creating connectivity

Creating connectivity is required at both the international and national fronts. Given the complexities of the SET base in Australia (and other countries), international collaboration, such as pursuing opportunities through the US TSWG, is most easily and effectively achieved if all agencies use a single connection from Australia.

#### Recommendation 3

The new SET unit will be the primary focus for international collaboration in SET counter-terrorism.

#### Accelerating good science

On the national front, the proposed SET unit should be tasked with creating a portfolio strategy around the inventory of identified SET projects. It would need to develop a pertinent ranking process that identifies the interaction of achievability, timeline and impact where relative ease of commercialisation/high impact has highest priority. Portfolio management should also address balance of research and technology for focus areas, needs and timing. This would assist the unit in better supporting collaboration with other countries.

The working group supports utilising existing expertise in assessing potential projects for funding in the ARC, NHMRC, cooperative research centres, CSIRO, DSTO, universities and industry. These organisations have considerable experience in measuring the quality of SET, understanding the track record of researchers and the issues relating to IP and have expertise in specific areas of SET. Funding agencies also have extensive databases that can be mined for potentially applicable projects.

Based on the response to the working group's e-mailed survey, **members agreed that a more comprehensive audit of Australia's SET base would form the basis of greater collaboration at the international level and be used as a driver of improving R&D**

**productivity in Australia.** Additionally, an audit would be a first stage in developing a collaborative platform in conjunction with the four Academies as described in the section on survey results. The working group believes that the collaborative platform should be established to actively stimulate participation in R&D relevant to counter-terrorism.

The working group suggests that the SET unit should put in place mechanisms for providing **adequate recognition for researchers and developers who make a contribution to Australia's national security.** Excellence should continue to be a fundamental for government funding / support of SET projects.

#### Recommendation 4

The unit will develop a portfolio management process for SET support for counter-terrorism via

- developing and maintaining a SET inventory for potential support of counter-terrorism
- promoting SET requirements and gaps
- establishing collaborative programmes and activities and recognition mechanisms

Following September 11, the tragic event in Bali and the likely ongoing risk of terrorist attack, the working group strongly recommends that research on national security be included as a priority theme.

#### Recommendation 5

National security included as a national research priority.

#### *SET support for biological threats*

A detailed analysis of the biological threat and recommendations on a way forward are provided in Appendix 5. Although this was outside the Terms of Reference of the working group, two working group members, Professor Sue Serjeantson and Dr Denis Wade, were eminently qualified to provide more detailed comments on this area. The working group supports the following suggestions:

1. Requesting proposals to integrate the available real-time data from general medical practices and from government agencies including the Health Insurance Commission and the Pharmaceutical Benefits Scheme.  
Techniques now exist to monitor the data for changing patterns of disease incidence or distribution and drug use. Much of the raw data is already in digital form.
2. Supporting research programs directed at the development of rapid, stable, diagnostic tests for likely biohazards. Ideally such tests would be stable, inexpensive to run, simple to use and not require expensive equipment.
3. Supporting the development of biosensor or other technology for the detection of biohazards in unopened packages including mail.

## Conclusion

The working group thanks PMSEIC for the opportunity to possibly contribute to Australia's national security and acknowledges the contributions made by all the agencies, organisations and individuals that donated their time to this project (see Appendix 3).

The value of these contributions is reflected in the collaborative work established through this working group with the following contributors: DSTO and CSIRO on critical infrastructure analysis; Geoscience Australia and Protective Security Coordination Centre on modelling; and University of Wollongong, the Attorney-General's Department, DSTO on analysing existing and potential counter-terrorism strategies.

Included in Appendix 6 are several promising examples of current SET projects underway in Australia that could support counter-terrorism activity. These examples illustrate the depth, breadth and diversity of current Australian R&D with potential counter-terrorism application. The projects deal with the following areas:

- Real-time detection of biological hazards
- Disaster victim recognition
- Face recognition
- Geological hazard assessment of urban communities
- Vulnerability assessment of buildings
- Detecting plastic explosives and other substances

## Glossary

ADF	Australian Defence Force	
AEEMA	Australian Electrical and Electronic Manufacturers Association	
AEMC	Australian Emergency Management Committee	
AFP	Australian Federal Police	
AGs	Attorney-General's Department	
AHA	Animal Health Australia	
ARC	Australian Research Council	
ASIO	Australian Security Intelligence Organisation	
ASNET	Australian Secure Network	
BSE	bovine spongiform encephalopathy	
CBNR	chemical, biological, nuclear, and radiological	
CBR	chemical, biological and radiological	
CCTC	Commonwealth Counter-terrorism Committee	
CI	critical infrastructure	
CIAC	Critical Infrastructure Advisory Council	
CIP	critical infrastructure protection	
CRC	Cooperative Research Centre	
CSIRO	Commonwealth Scientific and Industrial Research Organisation	
CT	counter terrorism	
CW	chemical warfare	
DEST	Department of Education, Science and Training	
DFACA	Defence Force Aid to Civilian Authorities	Governor-General call-out order required
DoD	Department of Defence	
DSTO	Defence Science and Technology Organisation	
EM	emergency management	
EMA	Emergency Management Australia	
EP	emergency preparedness	
FASTS	Federation of Australian Scientific and Technological Societies	
FMD	foot-and-mouth disease	
IAW	in accordance with	
MoU	Memorandum of Understanding	
NCBRWG	National CBR Working Group	
NCTC	National Counter Terrorism Committee	Responsible for the NCTP
NCTP	National Counter Terrorist Plan	

*This paper was prepared by an independent working group for PMSEIC. Its views are those of the group, not necessarily those of the Commonwealth Government.*

NHMRC	National Health and Medical Research Council	
PMSEIC	Prime Minister's Science, Engineering and Innovation Council	
R&D	research and development	
RFP	request for proposal	
SAC-PAV	Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence	Commonwealth/State counter terrorism committee (see NCTC)
SIDC-PAV	Special Inter-departmental Committee for Protection Against Violence	Commonwealth counter terrorism committee (see CCTC)
S&T	science and technology	
SET	science, engineering and technology	
TTCP	The Technical Cooperation Program	Australia, Canada, New Zealand, United Kingdom, USA
UAV	unmanned aerial vehicle	
US TSWG	United States Technical Support Working Group	
VLB	very large bomb	
VoIP	voice over internet protocol	using Internet Protocol to transport voice as an IP data stream
WMD	weapon of mass destruction	

## Appendix 1: Terms of Reference

In the light of September 11, 2001 and subsequent events, it is considered appropriate that PMSEIC receive a report which identifies Australia's science, engineering and technology support for combating terrorism and recommends practical ways for Australia's science, engineering and technology providers to contribute towards meeting Australia's current and future anti- and counter-terrorism needs.

The working group will prepare a paper and presentation for PMSEIC which:

- briefly outlines the current and future sectors potentially threatened by terrorism and describes possible directions and timeframes to develop effective counter measures
- audits and assesses current public and commercial science, engineering and technology capabilities to combat terrorism
- identifies opportunities for Australian public and commercial involvement in international science, engineering and technology initiatives in security
- recommends ways to harness Australia's science, engineering and technology base to our core security interests
- articulates a framework as the basis for facilitating science, engineering and technology collaboration on combating terrorism both nationally and internationally.

### Background

Defence against the asymmetric threat terrorism poses requires a national effort across a broad front of government (federal/state/territory), national bodies, the armed forces, industry and the science community. Science and technology can contribute to all phases involved in combating terrorism, namely, prevention, protection, response and recovery.

However, the existing environment for science, engineering and technology support to counter-terrorism is complex. There are a large number of organisations with the potential to contribute both as clients and as providers. There are also a variety of formal and informal domestic and international linkages in place. It is timely for PMSEIC to consider a report which sets the framework for future collaboration in science, engineering and technology and provides direction for policy makers on assessing potential threats and the timeframes for developing appropriate measures to counter those threats.

## Appendix 2: Membership of the PMSEIC Working Group on Science and Security

Member	Organisation
Mr Hutch Ranck (Chair)	Managing Director Du Pont (Australia) Ltd
Dr Tim McKenna, CSM	First Assistant Secretary Science Policy Defence Science and Technology Organisation
Dr Lynn Booth	Director, Strategic Analysis Policy Science Policy Division Defence Science and Technology Organisation
Dr Warren King	Chief Telecommunications & Industrial Physics Division CSIRO
Professor William Caelli	Head of School School of Software Engineering & Data Communications Queensland University of Technology
Professor Sue Serjeantson	Executive Secretary Australian Academy of Science
Mr Bernie McGeorge	Managing Director Zylotech Ltd
Dr Denis Wade	Chair & Managing Director Johnson & Johnson Research
Mr Richard Siebert	Manager, CT Capability Development, CT Branch, Protective Security Coordination Centre Attorney-General's Department
Secretariat	Department of Education, Science and Training

## Appendix 3: List of presenters to the working group

### Target / Method

Dr Gardner Murray	Chief Veterinary Officer
Mr Mike Nunn	Manager, Animal Health Science Department of Agriculture, Fisheries and Forestry
Mr Jonathon Potter	Chief IT Strategy Adviser CSIRO
Ms Veronica Borrett	Manager, Chemical Biological Radiological and Nuclear Domestic Preparedness Defence Science and Technology Organisation
Professor John Mathews	Deputy Chief Medical Officer
Professor Ross Babbage	Managing Director Strategy International (ACT) Pty Ltd

### Co-ordination / Linkages

Detective Superintendent Mark Johnsen	ACT Division Australian Federal Police
Mr Don Patterson	Emergency Management Australia
Mr Alex Webling	National Information Infrastructure Protection Committee
Mr James Carouso	Economic Officer US Embassy
Professor Rita Colwell	Director US National Science Foundation

### Solution Space

Dr Dennis Cooper	Ambri Limited
Mr Ron Cameron	Australian Nuclear Science and Technology Organisation
Mr Steve McIntosh	Australian Nuclear Science and Technology Organisation
Dr Julian Kelly	Australian Nuclear Science and Technology Organisation
Professor Vicki Sara	Australian Research Council
Dr Stephen Walker	Australian Research Council
Dr Stuart Shepherd	Australian Video Systems Pty Ltd
Dr John Schneider	Geoscience Australia
Dr Greg Scott	Geoscience Australia
Mr Jim Kennett	Parametric Technology Australia Pty Ltd
Mr Justin Aldrich	Parametric Technology Australia Pty Ltd

## **Appendix 4: SET survey e-mailed to private and public researchers**

Dear Colleague,

I am writing on behalf of the Prime Minister's Science, Engineering and Innovation Council (PMSEIC) working group on the topic of Science and Security. We are seeking information about current research projects being undertaken in Australia which have potential application to four phases in countering terrorism activities: prevention, detection, response and recovery.

We would appreciate it if you could fill out the short questionnaire below - it should take about ten minutes. Your response may be incorporated into a report being prepared by the working group for the November meeting of PMSEIC.

We need your reply by 20 September 2002. Please reply separately for each project if there is more than one relevant activity. Feel free to forward this e-mail on to anyone you know who may be involved in research potentially relevant to our national security; I apologise if this means you have received this e-mail more than once.

PLEASE MAIL RESPONSE TO: [President@science.org.au](mailto:President@science.org.au)

### Background

PMSEIC is the Government's principal source of independent advice on issues in science, engineering and innovation and relevant aspects of education and training. It is chaired by the Prime Minister and comprises Ministerial members, ex officio representatives of major science agencies and science and industry representative groups, and personal members. The Council meets twice a year and will next meet on 20 November 2002.

The agenda for the next meeting includes an item on Science and Security. An ad hoc working group has been appointed to address this issue. The Science and Security working group has been tasked with assessing the current public and commercial science, engineering and technology capabilities to combat terrorism. The terms of reference that are relevant to this request of the working group are below.

Your assistance is very much appreciated,

Thank you for your time,

Sue Serjeantson.

S.W. Serjeantson, AO,  
Professor,  
Executive Secretary,  
Australian Academy of Science,

Enquiries: Susan Wishart 0262405105

## Research with Potential Application to Counter-terrorism Activities Questionnaire

Name and Contact Details:

Project or instrument/facility name:

Project or instrument/facility description (no more than 5 lines):

What is the potential application to counter-terrorism activities (no more than 5 lines):

Time to commercial launch/operational readiness:

0-3 months       3-12 months       1-3 years       5 or more years

Equivalent full-time researchers (EFT) working on project:

1 person       2-5 people       more than 5 people

Total expenditure in this financial year (A\$):

Indicate threat categories to which your research is relevant by completing the matrix below –  
(Note: more than one box can be crossed)

Research Category	Area of Application	Prevention	Detection	Response	Recovery
<b>Capability Of Terrorist / Terrorist Group</b>	Personnel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Organisation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Facilities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Procedures	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Finance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Motivation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Methods*</b>					
Physical	Impact/kinetic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Explosive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Theft	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Hostage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Siege / Area denial	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Psychological	Propaganda	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Financial	Stock market	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Extortion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Criminal	Crime / social disorder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chemical	Land	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Water	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Air	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information	Intrusion / Monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Data corruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Denial of service/s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Destruction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Biological	Air	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Water	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Land	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Vector: human	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Vector: animal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Vector: plant	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Radiological	Release / Explosion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Nuclear	Detonation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Target*</b>					
People	Population centre	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Person	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Services	Finance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Security / Police / Emergency Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Information networks (incl cyber terrorism)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Food chain	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Energy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Water	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Tourism	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Health	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Education	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transport	Land	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Air	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Sea / Waterways	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Infrastructure	Government-Security / Defence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Industry -Defence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Industry-Chemical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Landmark	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Private	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\* the relationship between method and target is, for example, using IT (weapon) to sabotage the sewerage system (target).

## Appendix 5: Recommendations on SET support for biological threats

Although it is outside the Terms of Reference of the working group to suggest how Australia could better deal with specific aspects of terrorism threats, two working group members, Professor Sue Serjeantson and Dr Denis Wade, were eminently qualified to provide more detailed comments on biological threats. The working group provides their thoughts below for perusal of the Government. As the key word search on the NHMRC database primarily identified biological projects, the results have been included in table 3 of this appendix.

Whilst the use of biological agents as instruments of terror is probably less likely than physical weapons including explosives, modern techniques have made the use of biological agents a very real issue. The additional community chaos and alarm posed by the uncertainty about detection, containment and management has been well illustrated by recent 'white powder' threats in several countries including Australia. Importantly, the enormous problems associated with the decontamination associated with biological weapons has been clearly illustrated by the difficulties and recourses necessary to decontaminate the US government buildings after an exposure to small quantities of anthrax spores.

Modern techniques in microbiology and biotechnology have made the deliberate development of high virulence and other types of 'designer' organisms possible. Much of this technology is widely available in many countries and not beyond the resources of some terrorist groups.

The use of biological agents on any large scale does however pose other problems for the terrorist including quantity production, stability, distribution and self-protection. When all these issues are considered, it is clear that a consideration of 'what is a likely biological weapon' would probably produce a very different list from the list of 'what is possible'.

The working group agreed that the possible biological agents that could pose threats include:

- existing known pathogenic organisms and viruses, for example, anthrax, plague, smallpox, ebola, lassa fever, rabies, cholera and influenza;
- known toxins such as ricin or botulinum toxin;
- virulent strains of known pathogens. Virulent strains of influenza associated with low antibody levels to the virus in the community may be associated with widespread morbidity and considerable mortality not only in the elderly and debilitated;
- 'designer' organisms, viruses or toxins;
- possible biological threats, for example, 'white powders'; and
- pathogens with agro-economic targets, for example, foot-and-mouth disease.

Whilst all are possible, 'designer' bacteria, viruses and toxins are least likely for both biological and logistic reasons. The aims of the terrorist would seem to be achieved with much simpler agents.

### The response to a biological threat or attack

There are several key elements when responding to a threat of attack with a possible biological agent. These include:

- identifying that the possibility of a biological attack exists by real-time monitoring of the community. Whilst rare diseases or toxicity is readily identified, a change in the incidence of a common disease is usually not identified rapidly. Real-time epidemiological monitoring is now possible with available data and analysis techniques;
- rapid confirmation or exclusion of the possibility that a biological agent is involved. The need for stable, easily used, low cost tests to identify likely bacterial pathogens would aid response, facilitate containment and avoid unnecessary panic if there is no biological threat;
- rapid containment of the agent to limit spread;

- rapid community response;
- detailed identification of the agent;
- community protection to limit spread. Vaccination, passive antibody protection, antitoxins and drug antidotes are important with specific biohazards.

#### **Suggested support for SET directed at these problems**

The working group suggests that in relation to biological threats, consideration be given to:

1. Requesting proposals to integrate the available real-time data from general medical practices and from government agencies including the Health Insurance Commission and the Pharmaceutical Benefits Scheme.  
  
Techniques now exist to monitor the data for changing patterns of disease incidence or distribution and drug use. Much of the raw data is already in digital form.
2. Supporting research programs directed at the development of rapid, stable, diagnostic tests for likely biohazards. Ideally such tests would be stable, inexpensive to run, simple to use and not require expensive equipment.
3. Supporting the development of biosensor or other technology for the detection of biohazards in unopened packages including mail.

**Table 3: NHMRC key word search**

The NHMRC conducted, on behalf of the working group, a key word search of its grant management database on grants with a budget during or since the year 2000. All together there are 880 grants, of which 315 appear against more than one category. There are 565 unique application infectious diseases.

<b>Key word search</b>	<b>No. of NHMRC grants</b>
Air quality	2
Antibody protection	0
Bacteria, bacterium	74
Biotech	9
Biowar, bioweapon, bioterror	0
Contaminate, contamination	0
Infection, infectious diseases	296
Microbiology	11
Parasite, parasitic	39
Pathogen, pathogenesis	132
Specific diseases (anthrax, smallpox, etc)	8
Toxin, toxicology	89
Vaccine, vaccination	83
Vector	16
Virus, virology	121
Total	880

## Appendix 6: Case studies

### 1. Real-time warning of biological-agent attacks with an integrated biochemical detection and warning system

There is a real need to develop improved defenses against biological agent use, focusing on more effective detection systems as the key to providing advanced warning of an attack or mitigating the effectiveness of an attack.

Requirements for a detection system are:

- real-time detection to provide warning in time to avoid exposure,
- near-real-time identification to identify agents in time to treat casualties,
- collection of samples for independent verification of use to validate any response,
- being as compact and transportable as possible.

Thus, the system should be focused on deploying a particle-sizing technology that could discriminate biological particles from other background particles, technologies to concentrate the particles from air in order to increase the sensitivities of the detection and antibody or DNA-based identification technology that requires little maintenance and logistical support but with a high level of sensitivity and specificity.

The particle sizing technology that would be capable to distinguish particles that contain live organisms from most other respirable particles in air is already available at QUT (the International Laboratory for Air Quality and Health). A key element of the system is an Ultraviolet Aerodynamic Particle Sizer (UV-APS). The UV-APS at QUT is the first instrument of its kind at any university/research organisation in the world as only the US and Canadian Defence Forces up to date were able to purchase the instrument.

QUT is also the lead site for the CRC for Diagnostics and, together with QUT's Infectious Diseases Program, has developed both antibody and DNA technologies for ultra-sensitive and specific identification of organisms. For instance, the QUT developed FNC technology is being used by Orchid Biosciences to identify remains from the World Trade Centre tragedy.

Technologies to concentrate particles from air are been fully utilized and developed at QUT in various applications within the Environmental Aerosol Program.

All three parts of the system should be integrated with a central processor unit. The central processor unit should be capable to discriminate manmade biological aerosol particles from all other background particles in air, in order to detect extremely low levels (<25 particles/l air) without excessive false alarms. The project needs to be supported to accelerate the research and development into potential benefits of close integration.

#### *Contact Information:*

Prof James Dale,  
 Director of Research, Faculty of Science,  
 Queensland University of Technology  
 Phone: 07 3864 2819 Fax:07 3864 5100 Mobile: 0410 520 269  
 Email\_address: j.dale@qut.edu.au

### 2. Disaster Victim Identification

For disaster victim identification (DVI), Australia is bound by international protocols developed by the International Criminal Police Organisation (ICPO) and Interpol. The 65<sup>th</sup> general assembly of ICPO-Interpol, in October 1996, authorized the Secretary General "to adapt the DVI form and associated guide whenever appropriate, pursuant to technical developments and/or other professional needs in the field."

The international protocol requires that primary identification be provided, meaning that dental records, fingerprints or the DNA profile from a missing person must be matched with information from a deceased person. In the early days following the tragedy of Bali, the media and the Australian people did not understand this requirement, and headlines such as “Bring the bodies home!” may have caused undue distress.

For DVI in Bali, dental records were of primary importance. For fingerprints, floppy discs obtained from homes of missing persons were particularly useful, as computer discs tend to be personal and have been firmly grasped between thumb and forefinger.

The DNA-based DVI procedures were centred in the forensic laboratories of the Australian Federal Police in Canberra, with forensic technicians from all States coming to central laboratories to combine their expertise. The earlier agreement by the States, when signing on to CrimTrac, to use standardized DNA analysis machines and Profiler Plus kits from the U.S. firm Perkin Elmer Applied Biosystems, meant that State technical expertise was readily integrated.

DNA is extracted from personal items of missing persons, such as hair and tooth brushes, for matching with autopsy specimens. The DNA profiler kit in current use simultaneously amplifies nine short tandem repeat regions of non-coding (junk) DNA. In addition, gender determination is provided through a segment of the X-Y homologous gene amelogenin. The probability that DNA from two unrelated individuals matches by chance in U.S. Caucasians is 1 in 3.6 billion and in African Americans is 1 in 8 billion.

The Profiler Plus DNA kits overlap with those used by the FBI and Interpol, among others, a matter of increasing importance given the global nature of terrorism, but could be augmented to better suit Australian conditions. Perkin Elmer has made a generous donation of Profiler Plus kits to the AFP for Bali DVI DNA testing.

### 3. Face Recognition / Verification

CSIRO has developed automatic face recognition technology capable of rapidly matching a face to an image stored on a database. The technology uses standard PC hardware with a video camera for image capture. Image matching accuracy is over 95%.



Combining this technology with PIN numbers or other biometric identification, can provide substantially higher levels of security. Application areas include automated security access, secure computer access, time and attendance monitoring, retail and manufacturing surveillance and crowd monitoring.

Various features are extracted from the captured faces which allows each to be individually described by a compact 'Facial Features' vector. This compressed representation of a face enables the rapid comparison against other faces.

The system performs automatic real-time face recognition and when a match is found, the user is alerted through sound, a flash of colour, an email or even a custom command. When the system has found a similar face, a warning is generated suggesting that the user should further investigate the candidate. This is particularly useful where there are crowds or busy thoroughfares, since only matching, or similar faces are brought to the attention of the operator. The system also allows the user to match an operator-selected face against faces captured over days or even weeks, all within a matter of seconds. The user can then quickly review the matched faces' time and date stamps to determine what times that person was present.

It has been developed by CSIRO to meet the need for non-intrusive recognition technology at airports, casinos, gaming clubs and numerous other high-risk environments where discrete visual recognition enhances existing security systems.

*Contact Information:*

Shay Withnell

CSIRO Telecommunications and Industrial Physics

Phone 02 9372 4607 Fax 02 9372 4555

Email: shay.withnell@csiro.au

#### **4. Geological hazard assessment of urban communities**

Geoscience Australia (GA) is the national agency for geoscience research and geospatial information. GA provides input for decisions that impact upon resource use, management of the environment, and the safety and well-being of Australians. GA has strong science, engineering and technology (SET) capabilities that could be directed to counter terrorism activities. These include the National Mapping Division and the Commonwealth Office of Spatial Data Management. The Urban Risk Research Group, within the Minerals and Geohazards Division, co-ordinates the activities of the Cities Project, the Risk Modelling Project, and the Geospatial and Visualisation Group.

GA is unique in the way it can develop scenarios on the impact of a natural disaster based around spatial data analysis, risk modelling and inter-agency collaboration. The technique used by GA can be used to assist counter-terrorist planning by running multiple computer-simulated scenarios in one city, or across Australia, to determine key vulnerabilities, for example in health services or critical infrastructure. The technique can also be used to provide near real time estimates of losses to response managers to assist them to prioritise their actions.

- *Spatial data analysis* integrates information from a number of large disparate datasets in a Geographic Information Systems (GIS) environment. These datasets contain comprehensive information on buildings, critical infrastructure, population demography and economic activity. Collection and integration of these data on any city in Australia takes considerable time and requires access to datasets held by state departments, utilities, and local governments.
- *Risk modelling* provides computational models in many physical, engineering and socio-economic areas. They can include fluid dynamics models for explosion blast overpressures and thermal radiation, aerosol dispersion, the probability of casualties inside and outside buildings, economic losses incurred by building damage, as well as the broader social and economic consequences of an attack or an extreme event.
- *Interagency collaboration* is an essential part of this technique. In its natural hazard risk assessments GA's Cities Project has established extensive networks of collaborators at all three levels of government, the emergency management community, and with critical infrastructure agencies.

In most Australian cities it would take several months to obtain access to spatial data, and initiate and establish interagency collaborations. First-order estimates could then be produced of the consequences to selected urban locations or critical infrastructure, and an initial capability to assess the impact in response to a real event would be developed.

A more complete development of national capability to assess the risk of, for example, explosion or CBR attack, using the techniques of spatial data analysis and risk modelling could take several years to assemble. In addition, to ensure that the relevant spatial information was accessible and current, it would also involve establishing national research programs and international collaboration in the areas of blast modelling, aerosol dispersion and structural damage modelling.

*Contact Information:*

Dr John Schneider  
Group Leader  
Urban Risk Research Group  
Phone 02 6249 9667  
Email [john.schneider@ga.gov.au](mailto:john.schneider@ga.gov.au)

## **5. Vulnerability assessment of buildings**

Responding to the threat of terrorist attacks around the world, structural engineers are seeking and developing new methods and modelling techniques for assessment and prevention of damage to high-risk, Infrastructure and Landmark facilities, with the emphasis on severe blast, high impact and intensive fire. This concentrated R&D activity can deliver both short and long term benefits in enhanced security in Australia.

*Current Research Program in Australia*

In Australia the Research Group on Advanced Protective Technologies for Engineering Structures, was formed at the University of Melbourne in 2001. The main research theme of the group, (headed by Associate Professor Priyan Mendis), is to assess the performance and vulnerability of critical infrastructure, (Including major bridges, telecommunication centres, main power and water supply stations, landmark structures, commercial tall buildings, etc.) under both natural and technical hazards (accidents or terrorist attacks).

The objective is also to develop innovative and effective mitigation technologies for the protection of critical, high-risk facilities, from extreme events (blast, shock, impact, earthquake, etc.).

The group, using these evolving research and modelling techniques, has identified many weaknesses in our present design methods in Australia which can be taken into account in future construction.

On the short term benefit front, it has also identified that many methods used presently to strengthen structures in high seismic areas, such as FRP (Fibre reinforced Plastics), can be used/adopted to strengthen existing structures against terrorist loading. This work is continuing at the University of Melbourne.

*Advanced modelling techniques*

The powerful Finite Element Explicit Code LS-DYNA3D has been used extensively by researchers of the group to model transient dynamic problems such as blast and high velocity impact. So far, applications of this sophisticated code have been limited to the aerospace, car, and ship building industries, for impact and high velocity problems.

This package was designed in United States primarily for military purposes and is capable of simulating projectile penetration, blast response, and explosives. A new, constitutive model for concrete under high loading rates has been proposed by the research group to model concrete structures.

This sophisticated computer code has been used successfully in this recent research program funded by VPAC (Victorian Partnership for Advanced Computing) to model the potential damage to tall building structures in Australia under blast or aircraft impact. For details about this work see University of Melbourne media release (Sept 9<sup>th</sup> 2002, <http://www.unimelb.edu.au/news/>).

#### *Collaborative work*

The research group has been working closely with CSIRO and Australian Defence Force Academy (ADFA) as well as Protective Technology Centres in USA and Singapore. The group will actively participate in the tall buildings task force formed by World Council of Tall Buildings and Urban Habitat (CTBUH), CIB (International Council for Research and Innovation in Building and Construction) and NIST (National Institute of Standards and Technology, USA).

#### *Recent Event in Bali*

The group will gather information about the structural damage to the “open” structure (Sari Club) and evaluate the design methods used. A comparison will be done with the design methods and standards used in Australia for similar structures. This work will be conducted jointly with Prof. Benjamin Lumantarana of Petra University in Surabaya, Indonesia.

More Information; web site:<http://www.civag.unimelb.edu.au/seeg/apter>

#### *Contact Information*

<p>A/Prof. Priyan Mendis (<a href="mailto:pamendis@unimelb.edu.au">pamendis@unimelb.edu.au</a>) Reader in Civil Engineering Dept. of Civil &amp; Environmental Engineering The University of Melbourne, Victoria 3010 Tel: 61 3 8344 7244 Fax:61 3 8344 4616</p>	<p>Tuan Ngo (<a href="mailto:T.Ngo@civag.unimelb.edu.au">T.Ngo@civag.unimelb.edu.au</a>) Dept. of Civil &amp; Environmental Engineering, The University of Melbourne Victoria 3010 Tell: 61 3 8344 7950 Fax:61 3 8344 4616</p>
--	--

## **6. Detecting plastic explosives and other substances**

The rising threat of terrorism has increased the urgency for Thorlock International’s detection technology and know-how.

Based in Western Australia, Thorlock International Ltd employs about 30 staff most of whom are scientists and engineers. Over the last six years Thorlock has invested over \$18 million into research and development of an explosives detection system based upon Quadrupole Resonance (QR). QR is related to MRI technology which is widely used in medical applications.

QR identifies the molecular structure of a target through its unique radio frequency signature. QR can detect plastic explosives, narcotics, biochemical agents and pharmaceuticals.

Thorlock now has a product (T3000) that automatically and unambiguously detects plastic explosives to a level of accuracy that cannot be matched by currently deployed technologies. It will also cost substantially less to buy, install and maintain compared to existing systems being used to detect plastic explosives. The T3000 achieves significantly lower false alarm rates than the equipment currently in place while exceeding US and European regulatory requirements for detection.

Earlier this year the T3000 was approved as an Advanced Technology Explosive Detection System by the USA Transportation Security Administration (TSA) after being tested under a Cooperative Research and Development Agreement (CRDA). The US Federal Government entered into the CRDA with Thorlock as part of its Counter-Terrorism initiatives.

The T3000 has also been successfully tested by the UK Home Office, the Canadian Air Transport Security Corporation and at Ottawa, Manchester and Perth Airports.

Thorlock's world leading status was further confirmed recently when it was chosen over international competition to be granted a long term exclusive worldwide license by BTG PLC (a privatised UK government enterprise) over their extensive QR patent portfolio. BTG holds many of the vital patents covering MRI and first licensed MRI to General Electric in 1987.

Thorlock is receiving significant interest from international governments and major defence companies and is poised to become a major player in the Homeland Security and Defence industry by building on its achievements, its world beating technology and the leading QR R&D team. Thorlock will also advance QR technology into the development of the other applications and markets which are equally exciting and commercially lucrative.