



**ATTORNEY-GENERAL
HON ROBERT McCLELLAND MP**

**ADDRESS TO THE
NATIONAL SECURITY COLLEGE
SENIOR EXECUTIVE
DEVELOPMENT COURSE DINNER**

OLD PARLIAMENT HOUSE, CANBERRA

THURSDAY, 10 MARCH 2011

CHECK AGAINST DELIVERY

First, may I acknowledge the traditional owners of the land we meet on – and pay my respects to their elders, both past and present.

- Professor Michael L'Estrange, Director of the National Security College;
- Mr Roger Wilkins AO, Secretary, Attorney-General's Department;
- Mr David Irvine, Director-General of Security, Australian Security Intelligence Organisation (ASIO);
- Mr John Lawler APM, Chief Executive Officer, Australian Crime Commission;
- Mr Blair Comley, Secretary, Department of Climate Change and Energy Efficiency
- Assistant Commissioner Roman Quaedvlieg, ACT Chief Police Officer;
- Mr Frank Lewincamp;
- Distinguished guests, ladies and gentlemen.

It is my great pleasure to address you tonight as part of the Senior Executive Development Course at the National Security College.

Although only established last year, the College, under the leadership of Professor L'Estrange, is already establishing itself as a centre for leadership in the national security community. As well as developing excellence, the centre is a vital pivot in the creation of networks within and outside government.

The value of the Senior Executive Development Course, which is rapidly becoming the signature initiative of the College, is not only what you are exposed to and learn, but the networks you establish that will assist you in the future.

I understand you have discussed and considered issues across the national security space over the past few weeks. This evening, I would like to take the opportunity to speak broadly about the role of Government in protecting national security, the

current and emerging threat environment, and our proposed policy response and forward agenda.

An All-Hazards Approach to National Security

Of course, the first priority of Government is the protection of the safety and security of its citizens and its interests. However, what do we mean when we talk about 'national security'?

The Government's inaugural [National Security Statement](#) stated that national security meant:

'freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of our hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians.'

This broad approach recognises that, at any given time, there are many risks and dangers that threaten Australia's security – from espionage, terrorism, border violations, cyber attack, organised crime, natural disasters and biosecurity events.

These threats pose both security and safety risks, not only to Australia's institutions of state but also to its people, economic assets, infrastructure and technology.

While the security of our nation is a shared responsibility between governments, business and the community, Government obviously takes a key leadership role to protect the safety and security of Australians.

As Attorney-General, the national security responsibilities of my portfolio are broad – from counter-terrorism and emergency management, to border control and organised crime.

From this perspective, I am acutely aware of the importance of coordinated and integrated capabilities to address these diverse priorities buttressed by strong cooperative and coordinated relationships.

The Threat Environment

Our security environment is more fluid and interconnected than at any time in our history.

We live in a world where global factors have greater influence than ever before on the domestic front. Where change is more rapid and pervasive, and where things happen on a bigger scale and are communicated in real-time.

A prime example of these modern societal characteristics in action is the current upheaval in the Middle-East and Africa. Enabled by modern technologies such as Twitter and Facebook, the so-called 'Jasmine revolution' in Tunisia was very quickly followed by a groundswell of protest against a long standing and established regime in Egypt that resulted in sudden radical and significant change. We continue to witness similar significant ongoing protests in Libya and other nations elsewhere.

The effect of these momentous events will inevitably be felt in the Australian security environment.

Australia's counter-terrorism arrangements are, in many respects, quite mature. But the threat is enduring and its agility must be matched by ours.

The main terrorist threat continues to come not from State actors but from extremists who follow a distorted and militant interpretation of Islam. We continue to see the emergence of new groups and individuals inspired by the global jihadist

message as well as Australians continuing to attempt to travel overseas to train or fight.

Al-Qa'ida remains the most obvious, but not the only, manifestation of the global violent extremist movement. The al-Qa'ida network reaches far beyond its birth place, and is also linked to a range of other extremist groups.

While the majority of extremists operate in the context of an extremist group, there have been recent cases internationally of 'lone wolves' whose radicalisation and planning is often fairly simplistic and occurs in isolation without the knowledge even of their families and friends.

Terrorist tactics also appear to be evolving away from major shock attacks such as 9/11, to what's been described as 'the strategy of a thousand cuts' — where small-scale operations are judged by their would-be perpetrators as just as effective as large scale operations in terms of the consequential disruption.

Taken together, it is these two trends that are emerging with increasing frequency, that pose a particularly difficult challenge for our security agencies. To be frank, it is the main thing that keeps me awake at night.

Within the Australian security environment, we have also seen a trend in 'home-grown terrorism' with a very small abhorrent minority of Australians attracted to violent extremism.

Since 2001, 38 people have been charged with terrorism related offences in Australia. 37 of the 38 people charged are Australian citizens and 21 of the 38 were born in Australia. It is important, however, that we put this in context. The number of people attracted to terrorist ideology is in fact only very small. Nevertheless, their potential for harm is vastly disproportionate to their number.

Our security environment also needs to take into account our place in the world order.

The emergence of China will continue to be a dominant factor in Australia's foreign policy in the 21st century, whether you look at the impact of its resource requirements on our economy, implications of its relationship with the United States, or its increasing engagement in our immediate region.

While traditional threats like espionage and foreign interference remain significant, the explosion of the cyber world has expanded infinitely the opportunities for the covert acquisition of information by both state and non-state actors.

As these attacks can be staged from anywhere in the world, they can infiltrate the control systems of critical infrastructure, be activated remotely, causing damage and mayhem to our technology-dependant lives.

Public Policy Response

It's clear that the policy response to protect our nation needs to take into account these evolving threats and changes in our environment.

National Security Legislation

The first step is ensuring we have quality architecture. One of the key priorities of the Government has been achieving an effective and robust legal system.

The [National Security Legislation Amendment Act](#) which was passed in November last year, implemented significant reforms designed to ensure that our counter-terrorism laws are balanced and that our law enforcement and security agencies have the tools they need.

[Anti-people smuggling legislation](#), also passed last year made significant changes to strengthen our border protection regime, including enabling the Australian Security Intelligence Organisation (ASIO) to carry out its intelligence functions in relation to people smuggling and other serious border security threats. This has enabled ASIO to play a niche role in this area, with a focus on Australian links to people smuggling ventures.

Finally, just last week the Government passed legislation to enhance cooperation, assistance and information sharing between security, intelligence and law enforcement agencies.

The [Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010](#) will enable ASIO, the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO) to more closely cooperate and assist one another in support of key national security priorities.

The Bill also provides greater flexibility for ASIO to share intelligence and information with the broader national security community. It will also enable ASIO to cooperate with and provide assistance to law enforcement agencies in relation to telecommunications interception and other areas of expertise. This will support the National Interception Technical Assistance Centre, which enables ASIO to provide coordinated technical assistance to other Australian interception agencies.

Counter Terrorism

Counter-terrorism remains an ongoing priority.

The Australian Government's Counter-Terrorism White Paper, '[Securing Australia, Protecting Our Community](#)', released last year, brought together for the first time a

coordinated response to international and domestic terrorism, and articulated the Government's comprehensive, long term strategy on this issue.

Australia's law enforcement and intelligence agencies, along with the Commonwealth Director of Public Prosecutions, continue to work cooperatively in relation to counter-terrorism investigations.

Since 2000, there have been four disrupted terrorist plots in Australia. To date, 38 individuals have been prosecuted as a result of counter-terrorism operations and 23 have been convicted under the Criminal Code.

A key recommendation of the White Paper, the Counter Terrorism Control Centre (CTCC), was opened last year and represents an important development in the Government's counter-terrorism effort. The Centre, hosted by ASIO with representatives from key security, intelligence and law enforcement agencies, is playing a lead role in strengthening the coordination of Australia's counter-terrorism intelligence efforts. This is happening by managing counter-terrorism priorities, identifying intelligence requirements and ensuring that the process of collecting and distributing intelligence is fully integrated.

This level of coordination is essential to provide the best capability to detect and prevent terrorist threats to Australia and Australian interests.

The Centre shifts our well-coordinated counter-terrorism effort to a truly integrated one, and will strengthen Australia's national security capability by improving our ability to prepare for and respond to significant national and international threats.

Countering Violent Extremism

The Government also recognises that a comprehensive counter-terrorism response must include broader strategies to enhance social cohesion and resilience and lessen the appeal of extremist ideologies that fuel terrorism. We need to not only be tough on terrorism, but tough on the causes of terrorism. In essence, the old adage of prevention being better than cure is particularly relevant.

A key issue of concern is the risk of vulnerable individuals in Australia becoming radicalised to the point of being willing to use violence. Addressing this issue is a priority for the Government. Our goal is to help members of our communities to be less vulnerable to the process of radicalisation and violent extremism.

There is already a lot of valuable work being undertaken across the country at the State and Territory level. Countering violent extremism is, however, a national challenge that requires a national response.

It is this strategic direction that is being provided by the Government. As part of the 2010 Budget, we allocated \$9.7 million to addressing these issues. To lead this work, a dedicated unit has been established in the Attorney-General's Department to provide national direction and coordinate activities across Governments.

Effective community engagement is a key component of the Government's approach.

Communities have an important role in identifying and diverting vulnerable individuals before they come to the attention of security and law enforcement agencies. In order to support them in this role, the Government has commenced a series of regular meetings with community leaders around the country from a range of religious, ethnic and cultural backgrounds to listen and engage on these issues.

From these meetings I have learnt that there are a range of personal experiences that can make young people more vulnerable to extremist messages, for example:

economic issues such as a lack of employment opportunities, lack of education, discrimination and social isolation or marginalisation.

As a first step, the Government has sought to address some of these issues through our inaugural 'Youth Mentoring Grants' program. The grants provide funding for programs that directly support young people away from intolerant and radical ideologies and encourage positive participation in our community.

With nearly 100 applications, the Government received overwhelming interest in the program, reflecting the community's commitment to developing local initiatives to prevent extremism amongst our young people. Under the first round of this program, more than \$1.1 million has been committed for projects to support and mentor young people who are vulnerable to violent extremism.

In addition, the Government is also working to address the role of the internet in radicalisation. The promotion of violent extremism through the internet is becoming an increasingly concerning and visible threat, with the al-Qa'ida affiliated 'Inspire' magazine being a prime example.

Cyber Security

We live in a modern world. As we increasingly do business online, cyber security continues to be at the forefront of the Government's agenda.

Cyber intrusion, while a distinct method of accessing otherwise private information or disrupting critical systems, cannot be considered in isolation. It forms an important part of the broader security landscape. Ultimately, cyber security is a people problem – as people hack computers.

For this reason, we must continually invest in enhanced capabilities that will bolster our resilience to such threats. The 'Cyber Security Strategy' that I launched in November 2009 underpins the way in which the Government is seeking to achieve this.

CERT Australia — Australia's national computer emergency response team — is at the forefront of that response. Together with other Government agencies and a growing network of international partners, CERT Australia seeks to improve cyber security for all Australian Internet users and businesses. It places a special emphasis on assisting the owners and operators of systems of national interest — that is, those that, if compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.

CERT Australia works closely with the Cyber Security Operations Centre (CSOC), based within the Defence Signals Directorate (DSD), which focuses on identifying and responding to cyber incidents of national significance.

ASIO is also working to guard against foreign interference and espionage, including via technical means. This cooperation is crucial especially to countering the threat posed by those using the Internet as a modern espionage tool with the potential to facilitate access to large volumes of sensitive government and commercial information.

ASIO's close co-operation with CERT Australia and the CSOC seeks to identify developing threats and determine appropriate responses. For this reason, ASIO has also established a specialist cyber investigations unit to investigate and provide advice on state-sponsored cyber attack against, or involving, Australian interests.

Cyber activity is increasingly attracting considerable interest within the community. For example, work by the University of Toronto in 2009 uncovered 'GhostNet', which was believed to have infected computers belonging to Tibetan non-governmental organisations and the private office of the Dalai Lama.

Similarly, threats such as the 'Stuxnet' worm which worked by changing code in systems that control critical infrastructure and events in Estonia where an entire nation state was virtually brought to a stand-still by a sort of denial of service attack give an insight into the extent and capabilities of some hacking efforts.

These attacks and the threat to critical infrastructure such as banking, telecommunications and government systems is not something we can be complacent about.

The Government is taking active steps to improve international arrangements for cyber investigations. The Government has announced its intention to accede to the [Council of Europe Convention on Cybercrime](#) – the only binding international treaty on cybercrime.

Accession to the Convention is a critical step as it facilitates international co-operation between signatory countries and establishes procedures to make investigations more efficient. As such, it will help Australian agencies to better prevent, detect and prosecute cyber intrusions.

Emergency Management

I have often been asked 'why natural disasters are considered to require a national security response?'

Last week, I was in Christchurch with the New Zealand Minister for Earthquake Recovery Gerry Brownlee. He took me through the city's CBD which has been cordoned off by the police – a ghost town with crumbling buildings and bricks splayed across the roads. Urban Search and Rescue Teams from around the world – including Australia – continued to pick through the rubble. It felt almost like a war zone without the soldiers.

These kinds of catastrophic events – just like the recent floods and cyclone in Queensland - have shown that nature can be just as damaging as any man-made threat.

I put it to anyone asking this question that, it is our integrated crisis coordination and national security capabilities that our country depends on. Distinguishing between man-made and natural threats does not help us take the most coordinated approach to capability development about which I'll talk briefly in a moment.

Mitigation and ensuring our communities bounce back, and bounce back stronger, is therefore crucial. As a result, national security policy is increasingly focussed on the idea of resilience.

It is a concept that has been explicitly recognised by the Council of Australian Governments (COAG) as fundamental to enhancing Australia's capacity to withstand and recover from emergencies and disasters. Last month, COAG endorsed the ['National Strategy for Disaster Resilience'](#), which provides high-level guidance on disaster management and the development of disaster resilient communities.

The Strategy recognises that resilience is the collective responsibility of all elements of society – governments, business and the community— given their shared responsibility in preparing for, and responding to, disasters.

Forward Agenda

With a constantly evolving national security environment, we need to remain agile with the ability to foresee and respond to key threats and major developments. Improving our national security architecture and enhancing our capability remain the key priorities.

For example, the Prime Minister has commissioned an independent review of the Australian Intelligence Community to ensure our agencies are working effectively together and are well positioned for challenges in this constantly evolving security environment. The review is in full-swing, with consultations with intelligence agencies focusing on working arrangements, relationships and practices.

Recognising that the global security environment is increasingly complex and interconnected, we need to work ever more closely across national security agencies to ensure our capabilities most effectively address the risks we face. Our national security agencies have demonstrated an unprecedented level of coordination to help prevent and respond to threats to Australia's security. It is important that we continue this effort into the future.

Building on our Counter-Terrorism White Paper, the Government is developing Australia's first non-Defence National Security Capability Plan. The Plan will ensure all non-defence national security agencies agree on the security risks facing our country and the capabilities required to respond to those risks in the future.

The Government has also committed to developing a National Security Fusion Capability which will provide our border security, law enforcement and intelligence agencies with opportunities to expand and quickly link information to support the

fight against threats such as terrorism, espionage, cyber intrusion and organised crime.

Conclusion

The prominent UK intelligence professional, Sir David Omand defined national security as:

'...a state of trust on the part of the citizen that the risks to everyday life, whether from man-made threats or impersonal hazards, are being adequately managed to the extent that there is confidence than normal life can continue'.

Applying these expectations to our role, I am proud of progress the Government has made in protecting the safety and security of all Australians.

Obviously, we will continue to face challenges from a continually evolving national security environment. As such, we rely on you as our rising leaders in the national security community to be creative and flexible in meeting those challenges.

I have great confidence that you will.

Thank you.