RUSI of Australia Website Presentation Transcript

Politics of Defence – Australia's defence and security need

Ms Gai Brodtmann MP, Shadow Parliamentary Secretary for Defence spoke at the USI of the ACT on 5th November 2015.

The United Services Institute of the ACT hosted a presentation at the Australian Defence Colleges on the topic with two Canberra politicians, Senator 'Zed' Zeselja, and Ms Gai Brodtmann, MP. Ms Brodtmann's presentation is shown below in this transcript.

(USI Photo: The Hon. Senator 'Zed' Zeselja and Gai Brodtmann MP)

It's wonderful to join you tonight for this USI event – thank you for having me. I'd like to begin by acknowledging that we are meeting on the land of the Ngunnawal people, and to pay my respects to their elders, past and present.

I've been asked to speak about what I see are the issues of importance to Australia's Defence and security needs. Where do I begin? There are clearly many issues relating to Australia's Defence and security needs.

From the global spread of terrorism and intrastate conflict, the protection of our trade routes, maritime sovereignty disputes in the South China Sea, the prevention of threats such as people smuggling and organised crime, through to the security and defence implications of climate change.

With such a range of issues all worthy of attention I have decided to use the next 20 minutes to make some observations about two issues that have been of particular interest to me for some time: Sustainment and cybersecurity.

In the case of sustainment, it is an important issue that I believe receives far too little attention.

And in the case of cyber – despite the great amount of attention it receives – Australia is still behind the eight ball when it comes to action.

SUSTAINMENT

As I said, sustainment is a crucial issue that does not receive the attention it deserves.

Some facts, background and history:

- In the 2014-15 Budget, the Government allocated $6.3 billion on Acquisition, $6.2 billion on Sustainment and $0.1 billion on Provision on Policy Advice and Management Services.
- As a country, we spend almost as much on sustainment as we do on acquisition.
- I'll repeat that - as a country, we spend almost as much on sustainment as we do on acquisition. At any point in time, we have billions and billions of dollars' worth of military equipment under sustainment. Yet 'sustainment' seems to be treated as a word tacked on to the end of titles – or the end of reports.

How often do those of us in the defence community have heated debates about it? How often do you read media articles about sustainment? I would be willing to bet nowhere near as often as you would hear about acquisition – or ADF personnel – or deployments - or any other facet of Defence.

I've had a long running interest in sustainment after a decade of consulting for Defence and DMO - as it was known before its recent transformation into the Capability Acquisition and Sustainment Group

To me, effective sustainment is fundamental in achieving better results for the Australian Defence Force – and ultimately the Australian people. And proper public oversight of sustainment – including transparency and accountability - is a great means of ensuring effectiveness and value for money.

Proper public oversight - and this of course includes parliamentary oversight - enables public debate. Something which I believe is lacking when it comes to sustainment. Sustainment should be front and centre of any Government's approach to Defence.

Some history on sustainment:

After a review of the Collins Class Submarines was released last year, the General Manager for Collins Class submarine maintenance operations, Mark Stephens, said: *"The Coles report was a galvanising moment for ASC. It took us from doing two boats in full docking and changed that methodology. It has radically shaped how we look at the maintenance, what maintenance we do and how we do the maintenance."*

And in 2008 the Mortimer review recommended that DMO and Defence needed to further develop the key performance indicators in Materiel Sustainment Agreements and the systems needed to record sustainment performance and costs.

Between 2012 and 2014, the DMO, Navy and Army developed new performance measurement frameworks, including measures of availability, cost, schedule, and materiel deficiencies, which reported through a new DMO system. The new performance measures were developed to provide a firmer basis for the evaluation and active management of sustainment performance and costs.

However, their establishment remains at an early stage.

I find it surprising that only this year, in 2015, have performance measures been implemented that keep track of availability, cost, schedule, and materiel deficiencies. Defence does provide in various nooks and corners of its publications and online portals, information about sustainment.

Information on budget and expenditure data for the "Top 30 sustainment products" (representing some 77 per cent of current spending on sustainment) can only be found in an online only attachment to its Annual Report.

This attachment also includes an overview of the management of these products. While providing stakeholders with a basic summary of sustainment costs and activity, this information does not facilitate assessment of Defence and DMO's sustainment performance in terms of materiel availability, cost-effectiveness and key inputs such as inventory management, maintenance and configuration changes.

ANAO's 2015 report titled 'Materiel Sustainment Agreement' states that *'Defence still has some way to go before it meets the intent of the Joint Standing Committee on Foreign Affairs, Defence and Trade's recommendation for enhanced public reporting.'*

The reporting of the "Top 30" projects was far from prominent, and it invites an immediate comparison with the annual Major Projects Report provided annually to the JCPAA by ANAO and (now) CASG. This report goes into detail on major acquisition projects underway – it is a thick volume. But there is nothing comparable done for sustainment.

This is not to say that there should be an annual Major Sustainment Projects Report analogous to the MPR, though I believe it does no harm to discuss the question. But it does point out the need for a more systematic approach to transparency and oversight of sustainment.

We must keep in mind, as with any discussion of Defence matters, the need to be conscious of the security implications of public exposure of ongoing sustainment. But this does not prevent a more orderly and systematic presentation of information.

There is also a conceptual issue that I often find difficult to have addressed - "where does acquisition end and sustainment begin?" Although seemingly simple, in practice there doesn't seem to be a generally accepted characterisation. And I have found it puzzling that some platforms are very much in the operational phase, and yet they are still classed as being in the acquisition phase.

This fuzziness also makes it more difficult to unravel another key aspect of oversight: who is responsible for this platform right now?

My aim in making these observations is to start a discussion about sustainment – what it is, where it starts and how do we know that we are doing it well.

CYBER

Moving now to the second issue I want to talk about tonight – the threat posed by cyber-attacks. In contrast to the low intensity of public discussion about sustainment, discussion around cyber can be found everywhere: online, in the papers and in Government media releases almost on a daily basis. So we cannot say that this topic needs to be brought further into public debate.

But as I said earlier – despite all the talk – we've still got a lot of work to do. Cyber security has emerged over recent years as a substantial and growing challenge.

An increasing reliance upon the internet over the past decade has also created unexpected vulnerabilities. It's no longer some distant, emerging threat. It is here and now. It is our reality. As connectivity grows, so does the need for cyber-focused policies, legislation and regulatory frameworks.
According to the Australian Cyber Security Centre, cyber espionage can have a significant impact on Australia's national security and economic prosperity.

Much as cyber-attacks can be directed at any part of a country, we need to take a broad view of the implications for security. Attacks on fundamental infrastructure can seriously degrade national security.

As I speak foreign state-sponsored adversaries are targeting the networks of the Australian government (including state and territory), industry and individuals to satisfy requirements for economic, foreign policy, defence and security information, and gain advantage over Australia.

Australia is an attractive target for cyber espionage due to our:

- resource wealth
- range of commercial interests in Australia and internationally
- expertise in certain fields of scientific research, manufacturing and technology
- particular bilateral relationships and alliances
- prominent role in the Indo-Pacific region.

Significant compromises can also cause economic harm, damage Australia's reputation and undermine international and domestic confidence in Australian network security.

We saw this recently with David Jones – which had its computer system hacked and had customers' private details stolen. DJ's said a third party "exploited a vulnerability in its website".

Attacks like this are becoming increasingly common. According to Australia's Privacy

Commission, there has been a huge jump in reported data breach notifications in the 2014-15 financial year.

In 2014, CERT Australia - which is part of the ACSC - responded to 11,073 cyber security incidents affecting Australian businesses, 153 of which involved systems of national interest, critical infrastructure and government.

The threat cyber poses to our utilities is something I find particularly horrifying. Imagine this: Canberra has been out of electricity for a full day because the power grid is being held ransom by an international group of hackers, demanding money before electricity will be restored. It sounds like a scene from Batman, I know. But it could be a reality. This kind of attack on an electrical grid or water system could happen if critical infrastructure sectors don't improve their security systems.

In fact, it's already happening. According to the 2015 Global State of Information Security Survey, the utilities sector globally has seen the average number of cyber-crime incidents multiply by a staggering six times over the previous year – the most dramatic increase across any sector.

This poses a huge threat to our national security – and is not often considered enough in this context.

So how is Australia doing in the rapidly evolving national security theatre?

ASPI's International Cyber Policy Centre recently produced a report called '*Cyber maturity in the Asia-Pacific region 2015'.*

The report uses a 'cyber maturity metric' to assess the various facets of states' cyber capability throughout the Asia-Pacific – it analyses 20 countries. According to the report - 'Maturity' in this context is demonstrated by the presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations.
These cyber indicators cover whole-of-government policy and legislative structures, responses to financial crime, military organisation, business and digital economic strength, and levels of cyber social awareness.

ASPI has ranked Australia 5th in the Asia Pacific for cyber maturity. The United States placed first with a score of 90.7 out of 100, Japan second with 85.1, South Korea third with 82.8, Singapore fourth with 81.8 and we placed fifth – with 79.9.
I don't think we should be treating this as some sort of Olympics but while we are clearly doing well comparatively to the Asia Pacific region - there are obviously ways we could improve.

It really concerned me when I read that out of all the different factors Australia's cyber strategy was judged on – we scored the lowest in the categories 'Governance', 'Military' and 'Business' – which each received a score of 7 out of 10.

Under the Governance assessment it reads: *"Australia's score could improve with the release of a new cyber strategy and a more streamlined cyber policy structure to complement the country's operational cyber improvements."*

Under the Business assessment it reads *"there is a sustained two-way dialogue between government and key sectors such as banking, telecommunications and CNI. This effort could be both deepened and widened to incorporate more sectors."*

This is a fundamental ongoing issue: we need to ensure the smoothest flow of information between business and government seeing as cyber-attacks affect all sectors. But the assessment I find most concerning in ASPI's report, is of the military's role in cyberspace, policy and security.

The report reads: *"Australia's score remains unchanged from 2014. Australia also still lacks a publicly available strategy or policy document that guides the department's and the ADF's approach to cyber threats. The Defence Minister has indicated publicly that the upcoming Defence White Paper will look to address Defence's future cyber capability and the role it has to play in*

The aims of the RUSI of Australia are to promote informed debate, and to improve public awareness and understanding, of defence and national security. The views expressed by speakers are not to be regarded as being endorsed by the RUSI of Australia or its Constituent Bodies.

contributing to the protection of Australia and its critical systems. It also struggles to engage beyond traditional intelligence partners on cybersecurity issues. Australia's score could improve with further clarification of the ADF's roles and responsibilities."

This suggests that there are a number of questions we need to be asking ourselves:

- Despite the frequent news items, there still seems to be very uneven awareness among businesses, the private sector and even some public agencies.
- How do we lift the level of understanding and debate around cyber security?
- How should we develop capabilities to address modern elements of warfare, including in the cyber domain?
- What training do current members of the ADF need to combat these new challenges?
- And what are they currently receiving?
- How should cyber-related issues be incorporated into training for incoming personnel?
- Is ACSC appropriately funded and does it have staff with the required expertise?
- Is the ACSC linked up with Defence in a way that doesn't create silos?

There is another particular type of cyber threat that I'm also really concerned about – and comes under the category of 'cyberwar'.

Cyberwar can be classified as "*actions by a nation-state [or its proxies] to penetrate another nation's computers or networks for the purposes of causing damage or disruption"*

In the following remarks I would like to acknowledge the work done by an ANU intern in my office, Darian Clark, on a research project which has significantly improved my understanding of the issues.

Cyberwar represents a real and dangerous threat to international security.
It is clear that we have some way to go in the way we approach cyber.

But why? What is the urgency? The reason is that a cyber arms race is underway globally, with around 100 countries developing attack capabilities. We are in a brave new cyber world beset with ambiguities.

Cyber-conflict between states is real and happening and unless the use of cyber weapons can be checked, there is a risk that more frequent, enhanced forms of attacks may culminate in devastating outcomes.

The current situation has been compared to 1946 in the nuclear arms build-up, when states acquired potent new weapons but lacked the conceptual and doctrinal thinking to guide their use.

While there may be lessons from the Cold War period in terms of how states can achieve shared outlooks, the inherent nature of cyber weapons means that certain methods of arms control, like prohibition and compliance checks, appear to be redundant.

A significant part of the problem is the level of secrecy surrounding cybersecurity – this is creating much of the uncertainty among states.

As you can imagine – it is almost impossible to predict another nation's cyber capabilities or intentions as the virtual nature of cyber weapons makes them inherently covert.

For example, unlike nuclear weapons, cyber weapons can be produced in various settings, for different goals, and can be stored in a flexible manner that is almost impossible to detect through surveillance.

This is a major barrier to achieving a shared global cyber outlook – as nobody knows exactly what they're dealing with!

The ongoing absence of international consensus on how to restrain the use of cyber weapons, related to the challenges of how they operate, is the cause of much underlying instability in the global political system.

So what would such an agreement look like? One suggestion is to clarify sovereign accountability for national cyber territory and ban attacks on civilian infrastructure. Through the channel of UN negotiations, this offers a feasible way to mitigate the risk of cyberwar and minimise adverse effects during any such conflict.

We could also look at a comprehensive multilateral treaty. This could take the form of an 'International Convention to Regulate the Use of Information Systems in Armed Conflict'.

The precise form, at this stage, should be flexible – it is bringing parties around the table to map common ground that remains the fundamental priority. Once an initial agreement is in place – and that's the main concern here – this will leave open the door for the extension of future possible restraints.

I know that there are bilateral, plurilateral and multilateral discussions going on: I have heard for example that Germany and China are discussing a mutual no-hacking-for-economic-espionage pact, along the lines of agreements already signed between China and the US and UK. Normal signals intelligence and espionage remain OK however. The Government should be taking an active role in these discussions.

Conclusion

As I mentioned earlier, I don't have answers to all of the questions I have posed tonight – and there are many. They are questions that I will continue to discuss with the defence community as well as my parliamentary colleagues. And I look forward to our discussion tonight on these matters.

Biography:

Ms Gai Brodtmann MP was elected the Member for Canberra on 21 August 2010 and has extensive experience in the public, private and community sectors. Gai ran her own small business for ten years and understands the challenges faced by small business owners. Prior to that, she was a federal public servant, primarily with Foreign Affairs and Trade and Attorney-General's. Her public policy interests include education, small business, defence, foreign affairs, superannuation, financial literacy and public administration. In October 2013, she was appointed Shadow Parliamentary Secretary for Defence.

The aims of the RUSI of Australia are to promote informed debate, and to improve public awareness and understanding, of defence and national security. The views expressed by speakers are not to be regarded as being endorsed by the RUSI of Australia or its Constituent Bodies.