Intelligence, Information Technology and Cyber Programs

Andrew Davies

The 2009 Defence White Paper has much to say about military hardware, which has naturally captured the headlines, but there are also some initiatives that cover the enabling technologies and capabilities that allow the Australian Defence Force (ADF) to operate as a coherent whole and in a whole of government context. There is a discussion of the further development of intelligence, surveillance and reconnaissance capabilities and the networking of the ADF. Two major initiatives are an Australian-owned surveillance satellite and a new cyber warfare capability. Both of these have applications well outside of the defence domain and will present some challenges in their implementation. However, the White Paper discusses these initiatives in generalities only.

In the 2000 White Paper there was a significant focus on the 'knowledge edge', by which was meant that the Australian Defence Force (ADF) would have the training and systems in place to gain a warfighting advantage through a superior ability to gather, analyse and disseminate information. The 2009 White Paper reprises this idea, although not with the same emphasis.

This article provides an overview of some of the more significant announcements and ventures critiques of them, including risks and opportunities that can be identified. However, the White Paper is not much more than a statement of intent for the most part—there is almost no detail of what form the various initiatives will take, when they will be implemented or how much they will cost. For this reason, it is very hard to tell if the initiatives described are underpinned by realistic plans and strategies for implementation. In most instances, we will have to wait for more detail from the Defence Capability Plan or other sources.

Cyber Warfare

The government has included, for the first time, a section on cyber warfare in the White Paper. In many ways the White Paper description is not particularly illuminating, and notes that many of the capabilities will necessarily be highly classified.

After introducing the topic by way of warning of the threat to Defence, whole of government and commercial activities from cyberattacks, the paper says that the main new Australian capabilities will:

> consist of a much-enhanced cyber situational awareness and incident response capability, and the establishment of a Cyber Security Operations Centre to coordinate responses to incidents in cyberspace.
>
> The Cyber Security Operations Centre will include a continuously staffed watch office and an analysis team to respond to cyberthreats in a timely fashion. Its staff will include ADF and DSTO [Defence Science and Technology Organisation] personnel. This new Centre will be created within the Defence Signals Directorate (DSD), which already possesses significant cybersecurity expertise.[1]

Interestingly, there is no explicit mention of offensive operations in cyberspace. Nonetheless, it seems a reasonable guess that cyber operations will work both ways, and the paper hints as much when it notes that the new capabilities will "maximise Australia's strategic capacity and reach in this field".[2]

ADF personnel posted to the new centre will help it provide support to ADF operations, but the capability will be of service to the government more broadly. In order to achieve whole of government coordination, the Attorney General's Department and the Australian Federal Police will second staff to the centre. This will facilitate a response to cyber attacks across government and vital civilian infrastructure.

Overall, it is hard to assess the scope and significance of the new arrangements. It may well be the case that the government will be more forthcoming in a later publication, possibly originating from within the National Security apparatus being constructed under the Department of Prime Minister and Cabinet.

For now, the best guide might be the US Government's recently-announced Cyberspace Policy Review. This seventy-six page document discusses many of the issues that will also be relevant to Australia. It is also more forthcoming on what is involved in the US cyberspace initiatives:

> Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[3]

[1] Department of Defence, *Defending Australia in the Asia-Pacific Century: Force 2030* (Canberra: Commonwealth of Australia, 2009), para. 9.87-88.

[2] Ibid.

[3] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington DC: White House, 2009), p. iii.

As well, the US policy talks of a shared responsibility between the government and private sectors, including public-private relationships. International partners will also be engaged.

Defence's New Network

One Defence initiative announced after the launch of the White Paper that is relevant to a discussion of cyber warfare is the Defence Information Environment (DIE)—a major redevelopment that will see Defence move to a single network. Intended to provide savings through increased efficiency in the delivery of Information Technology (IT) services to Defence establishments, the

> Defence Information Environment will be one network connecting fixed and deployed locations built on a single set of standards and products. It will encompass all security levels and will determine that the right person has the right authority to access information. A typical desktop set up available to all Defence sites will be a single screen connected to a wireless network that can display multiple security sessions. Secure voice and video will be available to the desktop in most fixed and deployed locations.
>
> Deployed commanders and decision makers will have a single view of the battle space through a Common Operating Picture accessing a wide range of data from sensors and sources.[4]

This is an ambitious project. In fact, given the size of the task, the above extract can best be regarded as a 'vision statement' that will take years and considerable resources to implement. That is the charitable view. There is a more pessimistic assessment that could be made. This would not be the first 'one system suits all' IT project to turn out to be far more expensive and technically challenging than first envisaged. And this is not just a high-bandwidth wide-area network. The vision involves fusing data from disparate information sources and at different security levels. Given the difficulty Defence has had in implementing some of its previous data fusion projects—the much-delayed Project Vigilare in the air domain comes to mind—there has to be a serious question over the size and timing—or indeed the reality—of any savings that are ascribed to this project.

And the decision to have all security levels on the one network—and a wireless one at that—is an interesting one given the concerns about cyber security and recognition of cyber exploitation opportunities that seem to underpin the cyber warfare initiatives. In the past, networks carrying the most sensitive classified information were kept physically separate from other networks and/or secured by high-level encryption. This layered approach to security was intended to make physical access difficult, and to limit the opportunity for exploitation of any data that was obtained.

[4] Department of Defence, *The Strategic Reform Program 2009* (Canberra: Commonwealth of Australia, 2009), para. 108-109.

Since access to the World Wide Web will presumably be one of the services provided to Defence personnel, the move to a single DIE is, in the best case, a remarkable vote of confidence in the hardware and software security to be employed. At worst, it is a case of the IT efficiency tail wagging the operational security dog.

An Australian Satellite Capability

Many of the capability initiatives in the White Paper were flagged in advance, either through speeches by officials or by virtue of already being in the extant Defence Capability Plan. But there was one genuinely new announcement; Australia will be getting its own surveillance satellite.

The mooted satellite is “most likely to be based on a high-resolution, cloud-penetrating, synthetic aperture radar” (SAR).[5] The benefits of such a system are many. A SAR operating from low Earth orbit can systematically surveil a wide expanse of ocean or land, and automated recognition algorithms can be employed to search for surface targets at sea, for example. The return on investment can be competitive with other systems, such as the US Global Hawk unmanned surveillance aircraft.[6]

The White Paper notes that the Jindalee Operational Radar Network (JORN) will continue to be progressively upgraded. But, capable as it is, JORN will always depend on vagaries of the ionosphere, and will at times provide a reduced coverage. Satellite-sourced data will be able to fill in some of the gaps. As well, ‘ground-truthing’ of returns is very important for producing accurate location data from JORN. The ability of a satellite to provide accurate fixes on targets also visible from JORN will allow for more accurate localisation.

An unanswered question in the White Paper is why Australia needs to be a satellite owner, rather than a customer of other providers or a contributor to allied systems. The recent decision to buy into the US-owned Wideband Global System (WGS) satellite constellation for high-bandwidth communications provides a possible model.[7] In that case, Australia decided not to ‘reinvent the wheel’ by developing and/or launching its own satellite.

Instead, Australia will fund a sixth satellite the existing WGS constellation, thus avoiding the cost, risk and delay inherent in research and development projects. And, as a result of building on an existing system, Australia will get worldwide communications coverage.

[5] Department of Defence, *Force 2030*, para. 9.80.

[6] Andrew Davies, *Around the world in ninety minutes—what an Australian satellite surveillance system could do*, ASPI Policy Analysis, no. 42 (Canberra: Australian Strategic Policy Institute, 2009).

[7] *Operational Wideband Global Satellite Communications Capability Obtained*, Parliamentary Secretary for Defence Procurement Press Release, Canberra, 3 June 2008.

The US also operates a large number of satellite-based surveillance assets, and Australia has access to much of the collected data through long-established intelligence sharing relationships. Opportunities similar to the WGS investment presumably exist in the surveillance world. By deciding on an indigenous Australian capability, the government may have decided that sovereignty issues—there is no question of who gets first priority for tasking of an Australian-owned system—and/or spin-off benefits to Australian industry make the investment worthwhile.

Situational Awareness, ISR and Electronic Warfare

Collecting data is relatively easy. Gathering it from multiple systems, deconflicting, fusing and making it available in a timely manner to all of the agencies that need to use it is more challenging, but that is where much of the 'value added' lies.

The White Paper recognises the value of a common operating picture that draws on information collected by Defence-owned and non-Defence sources. As noted above, the DIE is intended to provide a single point of access for all such information. There is little detail provided and it is therefore hard to evaluate the proposal. The best that can be said is that the aim of moving to standardised protocols and standards is a welcome one—it is just to be hoped that those standards will be compatible with the fast-moving commercial IT world, and not be bespoke solutions.

Consistent with the focus in Defence publications over the last few years, the networked future force receives a few paragraphs worth of attention. However, the best that can be said about the very general statement included is that it recognises the project challenges and hints at a suitable 'spiral development' path:

> The development of such a force presents new challenges in the way Defence manages projects that deliver capability and will require significant coordination, cross project collaboration and industry liaison. It will also need the support of a comprehensive joint training and education program and a clear master plan with key milestones.
>
> The Government has confirmed that Defence is to build a networked ADF, and that it will achieve this by way of progressively delivering networked maritime, land, air and ISR [Intelligence, Surveillance and Reconnaissance] domains.[8]

There is also a hint that there will be a more detailed plan produced, which will include some development milestones.

Despite Australia deciding to get into the satellite ownership business, it continues to be the case that the United States will continue to develop,

[8] Department of Defence, *Force 2030*, para. 9.95–96.

deploy and operate surveillance assets on a scale that Australia cannot hope to emulate. The White Paper recognises this, noting that

> [Australia] will [improve] ISR linkages with the United States, especially in the wider Asia-Pacific region covered by the US Pacific Command … improving our capability to gather and share information from a wide range of sensors. This initiative has the potential to improve the visibility of activities in our maritime approaches and across the region through the sharing of surveillance information and capabilities. Increased investment in ISR cooperation with the United States will allow us to boost our ISR capability and contribute practically to the deepening of our already strong alliance relationship.[9]

A recent trend towards 'off-the shelf' acquisition of major platforms will bring the benefit of interoperability with the parent services (in the case of the Super Hornet, for example, with the US Navy). In fact, it will sometimes be the case that interoperability with corresponding allied services will be easier to implement than between Australian services.

Given the centrality of electronic warfare (EW) to modern warfighting, it is heartening to see this recognised in a further consolidation of the ADF's electronic warfare capability. A joint EW centre, collocating a number of ADF EW units, will be established, "probably" located in Adelaide.[10] This announcement is not new in itself, being essentially a further consolidation of the idea behind the 2002 establishment of the Joint EW Operational Support Unit (JEWOSU).[11]

The JEWOSU was formed through the amalgamation of the Air Force Electronic Warfare Squadron and Navy Electronic Warfare Support Division. Elements of the Army's EW capability will presumably come under the new centre as well.

Given the electronic warfare capabilities currently in the acquisition pipeline (the Air Warfare Destroyers, F-35 Joint Strike Fighters, possibly the EF-18G *Growler* variant of the *Super Hornet* and other capabilities under the auspices of Project DEF 224 *Bunyip*), the development of a truly joint unit will allow for a 'critical mass' of expertise to be built. This will be especially important in the analytic support area—EW is something of a 'black art' and it takes time to develop high levels of skill. In this respect, the ADF's biannual posting cycle will present a challenge. The civilian expertise of DSD and DSTO will therefore be an important part of the national capability.

[9] Ibid., para. 9.84.
[10] Ibid., para. 9.92.
[11] 'New joint electronic warfare unit formed', *Air Force News*, 18 July 2002, available at <www.defence.gov.au/news/raafnews/EDITIONS/4413/story07.htm> [Accessed 11 June 2009].

Conclusion

While not attracting the media attention of the big-ticket military platforms, the enabling technologies described in the White Paper under the general heading 'Information Superiority' will, in many ways, be the key components of ADF and national capability. The trick will be to turn some of the more ambitious statements into reality. The recent history of projects designed to produce a highly-networked force has been somewhat patchy.[12] Hopefully some lessons have been learned and a general approach of spiral development and leveraging off established technologies and standards will be the order of the day.

Andrew Davies is a theoretical physicist by training, and held postdoctoral positions at the University of Melbourne and the Australian National University. He joined the Analytic Studies Group in the Department of Defence in 1994. He worked on a range of scientific studies in support of Defence decision making, including submarine detection for the RAN, Army firepower options and RAAF stand-off weapons effectiveness. He led the Capability Analysis Branch within Defence Headquarters for a time, before moving into the world of signals intelligence and information security with the Defence Signals Directorate. Andrew joined the Australian Strategic Policy Institute as director of the Operations and Capability Program in 2006 and has written extensively on ADF capability and defence acquisition decisions. AndrewDavies@aspi.org.au.

[12] Douglas Abdiel and Andrew Davies, *ADF Capability Review: C^4ISR(EW)*, ASPI Policy Analysis, no. 30 (Canberra: Australian Strategic Policy Institute, 2008).