Inquiry into Defence Legislation Amendment (Security of Defence Premises) Bill 2010

Reference: A. Senate Standing Committee on Foreign Affairs, Defence and Trade letter to Professor Hugh White of 5 July 2010.

Senate Standing Committee on Foreign Affairs, Defence and Trade

I assume you have, or will have, a detailed submission from the Defence Security Authority on this topic.

I was asked by Professor Hugh White, Head of the Australian National University's Strategic and Defence Studies Centre, where I am a Visiting Fellow, to provide some relevant observations in response to Reference A.

My brief comments are based upon my experience as Director of Security Intelligence in Defence during 1998-2002 and, since then, working as an academic on national security issues.

The main security threats to Defence bases, facilities, assets and personnel in Australia, in my view, in order of concern, have been:

Theft by both insiders and external parties of attractive, valuable or hard-to-obtain items kept and stored at Defence facilities. Such items can include night vision devices, operational military equipment, weapons and ammunition, and military ordnance and explosives. An ongoing concern at some Defence facilities is the potential for an organised attempt to gain access to weapons and explosives. (For safety reasons, explosives are often stored in isolated bunkers.)

Cyber penetration of Defence systems to achieve intelligence collection or to test our cyber defences to gain a future operational advantage. The most likely nation to engage in such activity is China.

Terrorism, particularly by Australian home grown extremists. Such extremists are motivated by our ADF involvement in Afghanistan, and Australia's political support for the US and Israel. At least three of the Islamist extremist terrorism cases in Australia since 9/11 have involved plans for attacks on Defence facilities using explosives or firearms.

State espionage focussed on operational activities at some Defence facilities - particularly where there is a joint operational intelligence activity with another allied nation state, as at Pine Gap, or where other types of intelligence activities are conducted. The most likely nations to engage in such collection activities are China and Russia.

Attempts to gain access to advanced Australian and allied Defence research through areas such as DSTO and Australian Defence industry, mainly to gain commercial advantage, but could also include nation state activity for strategic benefit. Again the main threat comes from China - but a range of nation states is interested in gaining information for commercial or strategic advantage.

Sabotage and vandalism by disaffected elements, both within and outside the ADF. This could include deliberate tampering with military equipment to make it unserviceable.

Attempts to subvert Defence military and civilian personnel to get them to assist with some of the above activities.

In relation to preventing or safeguarding against the above security threats, some further observations:

Theft

It is important that all attractive items be adequately secured and accounted for on a regular basis.

Problems have been created at Defence facilities in the past by the Department of Defence contracting guarding services to civilian contractors who did not have a right of search, and Defence facility managers allowing employees' civilian vehicles to be parked near storage facilities, facilitating the theft of larger attractive items.

Adequate personal security-screening of the large number of civilian staff employed at some facilities has been a problem. The same has been true of transient contract staff, such as cleaners.

Relying on the integrity of trusted individuals working on their own can be problematic, as was demonstrated by a trusted army officer's theft in 2007 of eight or more M-72 LAWs (the exact number is still not known) for sale to interested parties. Most of the stolen M-72s are believed to be in the hands of Australian criminals and/or extremists.

Back-to-base overt *and covert* monitoring systems (both electro-optical and non-electro-optical) can be used to provide additional protective security, but they should be linked to a response group at the Defence facility. (Past experience has shown that it is imprudent to rely on a timely local civilian police response.)

It is important that recorded electronic data be made available to any court trying offences that have been monitored electronically. (Note that there are many surveillance systems that are not optical.)

Guard staff at all Defence facilities should have the power to search all persons and vehicles that enter or leave the facility. This should be a condition of entry.

Cyber penetration

Cyber attack is of course a growth area of concern. Defence now has a Cyber Security Operations Centre (CSOC) to monitor and protect against external attempts to penetrate Defence systems.

Stand-alone IT systems with air gaps provide a measure of protection, but there are ways in which even stand-alone systems can be accessed or compromised – as the recent Wikileaks case has shown.

Socially engineered attacks to obtain or compromise information about an organization or its computer systems are now a common occurrence. Aggregation of data from social networking sites is a way of gaining access to Defence employees and gathering data for socially engineered attacks.

Good cyber security relies on safe security practices by staff, and maintaining a high level of security for networks and data, with regular third party auditing of electronic systems.

Terrorism

It is not practical to provide effective perimeter security fencing at most geographically large Defence bases. Trespass legislation is therefore an important means of ensuring that such facilities can limit and control external access.

Legislation should include safeguards to prevent persons from loitering outside and imaging Defence facilities - which could be surveillance in preparation for a terrorist attack.

In the event of a terrorist or other violent attack, it is important that Defence or security personnel be able to respond quickly with lethal force in order to save lives.

The November 2009 US case of Major Hasan at Fort Hood (who disagreed with the US's involvement in Iraq and Afghanistan, and killed 13 fellow service personnel) shows that violent threats at Defence facilities may not be limited to outsiders.

Nation state espionage

China tends to rely on intelligence collection at facilities of interest by exploiting employees of Chinese background. China does not usually require them to collect security-classified material, but rather to seek out and provide unclassified material that is not in the public domain. This makes prosecution difficult.

It is therefore important that information that could be of interest to foreign nation states be adequately protected. We should probably have a more comprehensive protective classification for government-related unclassified information - as the US does with its “For Official Use Only”.

Russia tends to rely on technical collection against Defence facilities. This may necessitate gaining close proximity to areas of interest. New security legislation should include move-on provisions to prevent persons from loitering outside Defence facilities, particularly ones that are intelligence-related.

Several countries remain interested in cultivating human intelligence sources with Australian Defence access.

All types of potential intelligence collection activity need to be highlighted to staff by regular security awareness programs, citing recent examples of security vulnerabilities.

A further category of security concern is that of trusted insiders who attempt to gain some personal advantage by providing security classified material to others - as with Defence’s cases involving Jean-Philippe Wispelaere in 1999, and Simon Lappas in 2000.

Attempts to gain access to advanced Australian and allied Defence research.

Problems in this area can be reduced by limiting the number of personnel having access to such areas, diligent security vetting, exercising need-to-know and compartmented access controls, properly securing sensitive research material – including unclassified official material, and having an ongoing security awareness program.

Sabotage and vandalism.

Sabotage is more likely to occur if ADF activities and deployments are contentious both within and outside Defence. (I am not aware of sabotage having been a problem in recent years, but it was a problem in Australia during the Korean and Vietnam wars, and could conceivably become a problem in the right circumstances in the future.)

This situation may be avoided by adequately securing important sabotage-able items, and regular checking of stored items.

Vandalism is a potentially costly nuisance offence. It can largely be avoided by having roving security personnel at Defence facilities, particularly where trespass has been an ongoing problem. Back-to-base monitoring systems can also be used to provide additional security for buildings and items that tend to be vandalised.

Trespass at Defence facilities should be a detainable offence, with adequate penalties provided through civilian courts - with substantial penalties for repeat offenders.

Attempts to subvert Defence security

All staff should be made aware of the need to report to their security officer any incidents of concern involving Defence facilities or personnel - or attempts to solicit information about their employment or fellow employees.

Security of Australian Defence facilities and premises overseas

These are a special case; requiring assessment based on the nature of local security threats.

Conclusions

The Defence Legislation Amendment (Security of Defence Premises) Bill 2010 should include measures that provide appropriate protective security safeguards for all Defence premises, taking into account some of the protective security issues listed above.

These measures should include:

- **Personal security screening of all civilian staff, including contract staff.**
- **Monitoring of trusted insiders engaged on particular types of activity.**
- **Clarification of trespass offences and arrest powers.**
- **Provision for providing electronic monitoring data to law enforcement agencies, and Commonwealth, State and Territory public prosecution authorities, where appropriate. (Availability should not be limited to overt optical surveillance devices.)**
- **Guard staff having move-on powers for persons loitering outside Defence facilities.**
- **Guard staff being armed - or having ready access to firearms.**

- **Provision, in-extremis, for appropriately trained ADF or civilian personnel to use reasonable and necessary force, including lethal force, to safeguard persons and property at Defence facilities.**

- **Guard staff having the power to search all persons and vehicles entering or leaving Defence facilities.**

- **Providing better security protection for attractive items, including official information that is not currently security classified, and military ordnance - to protect against unauthorised removal from Defence facilities.**

I would be happy to provide further information if necessary.

Clive Williams
Strategic & Defence Studies Centre
The Australian National University

30 July 2010