10

Challenges

10.1 The Committee is aware of new challenges faced by Defence, due to the changing profile of security threats. In a number of instances these are generated by both state and non-state actors, ushering in a new, complex defence environment.

10.2 There were three matters which formed the basis of the Committee's questioning in this area:

- Defence's involvement in the Proliferation Security Initiative (PSI);
- Defence's readiness to respond to radiological threats; and
- Defence's preparedness for cyber warfare threats.

Defence's involvement in the Proliferation Security Initiative

Introduction

10.3 The Committee asked Defence to describe its current engagement with the PSI, a 'means of cooperating to prevent illicit trafficking in weapons of mass destruction'.[1]

10.4 PSI institutes cooperative arrangements between partner countries and provides an overarching layer for regional counter proliferation engagements, as well as training, preparation and response to radiological threats. Participation in PSI entails signing up to the Statement of

---

1 Department of Foreign Affairs and Trade, *Proliferation Security Initiative*, viewed 11/06/09, http://www.dfat.gov.au/globalissues/psi/index.html.

Interdiction Principles (SIP), and participation in training and exercises. 'More than 90' countries are involved.[2]

Anticipated threats

10.5 The Committee asked Defence to detail current anticipated threats from Weapons of Mass Destruction (WMDs) to Australia and the region. Defence advised the Committee that:

> The proliferation of Weapons of Mass Destruction (WMD) is, and will likely remain, a security issue of concern to Australia. The number of states with WMD, or with a 'break out' capability to rapidly produce WMD, is growing due to increasing industrialisation in the region. Moreover, terrorist groups have expressed a desire to acquire WMD. Proliferation networks have, in the past, been active in the region, and inadequate export controls means that the region is likely to remain attractive to proliferators. [3]

10.6 In response to these threats, Defence told the Committee:

> Law enforcement, counter-proliferation and export control regimes, and security assurances up to and including US extended deterrence will likely remain features of the region's response to such risks.[4]

Greater detail on PSI

10.7 The Committee asked Defence for greater detail on PSI and the Statement of Interdiction Principles. Defence advised the Committee that:

> PSI creates a framework for practical international cooperation to combat the illicit transfer of WMD, delivery systems and related materials.[5]

10.8 On the SIP, Defence advised the Committee that, it served to build upon:

> … participants' existing defence, enforcement, intelligence and diplomatic capabilities consistent with domestic and international

2 DFAT, *Proliferation Security Initiative.*
3 Department of Defence, *Submission no.2*, p.1.
4 Department of Defence, *Submission no.2*, p.1.
5 Department of Defence, *Submission no.2*, p.1.

> law – to deter, interrupt and interdict the transhipment of WMD materials.[6]

10.9 Defence advised the Committee that obligations pursuant to signing the SIP, were such that participants committed to:

- 'Undertake effective measures, either alone or in concert with other states, for interdicting the transfer or transport of WMD, their delivery systems, and related materials to and from states and non-state actors of proliferation concern';
- 'Adopt streamlined procedures for rapid exchange of relevant information';
- 'Review and work to strengthen their relevant national legal authorities';[7] and
- 'Take specific actions in support of interdiction efforts regarding cargoes of WMD, their delivery systems, or related materials, to the extent their national legal authorities permit and consistent with their obligations under international law and frameworks.'[8]

Support for PSI

10.10 The Committee also asked how involved Defence is in PSI; whether Defence could advise the Committee of instances where the SIP had have come into play; and had PSI scenarios emerged that were not covered by the SIP?[9]

10.11 Defence advised the Committee that Australia had continued strong involvement in, and support for the PSI since its inception by the United States in 2003.

> Defence is actively involved in the PSI, including through annual international meetings of the OEG (the Australian delegation is led by Defence), workshops and multilateral exercises.[10]

10.12 The depth of Defence's involvement with PSI is indicated by its record in supporting the Initiative:

---

6 Department of Defence, *Submission no.2*, p.1.
7 Department of Defence, *Submission no.2*, p.1.
8 Department of Defence, *Submission no.2*, p.2.
9 Department of Defence, *Submission no.2*, p.2.
10 Department of Defence, *Submission no.2*, p.2.

> Defence has been extensively involved in all of the activities hosted by Australia including two Operational Experts Group (OEG) meetings (in 2003 and 2004) and two PSI exercises (in 2003 and 2007). Defence has supported PSI exercises in other Asia-Pacific countries (eg New Zealand, Singapore and Japan) with ships, aircraft and specialist personnel.[11]

10.13 Defence described in greater detail the specific kinds of support it provides within the cooperative framework of PSI:

> The Australian Defence Force (ADF) provides support to Australia's PSI activities through the provision of assets to PSI tasks, advice to the Government on PSI matters and liaison/training with other government departments and other nations supporting the PSI.[12]

10.14 In response to the Committee's question on events falling within the remit of PSI, but outside the boundaries of the SIP, Defence advised the Committee that this had not occurred.[13]

Radiological threats

10.15 The Committee asked Defence to provide information on its preparedness and participation where radiological threats are anticipated. Specifically, the Committee asked Defence to advise it on:

- Defence's assessment of the current and future levels of radiological threat for Australia and its region;
- Whether units of the ADF are routinely equipped, trained and exercised in anticipation of radiological threats;
- Which other services would be involved, should a radiological threat emerge, and whether Defence conducted regular exercises with these services with respect to radiological threat scenarios; and
- Whether there had been instances where this capability has been brought into play due to radiological threats, whether anticipated or actual.[14]

---

11 Department of Defence, *Submission no.2*, p.2.
12 Department of Defence, *Submission no.2*, p.2.
13 Department of Defence, *Submission no.2*, p.2.
14 Department of Defence, *Submission no.2*, pp.3-4.

Relevant functions

10.16 Defence advised the Committee that the Defence Intelligence Organisation (DIO) 'conducts classified intelligence assessments relevant to the defence of Australia and its interests'. As a function of this, DIO:

> …routinely provides assessments relating to Chemical, Biological, Radiological and Nuclear (CBRN) threats to the ADF, and in support of whole-of-government counter terrorism and counter proliferation efforts.[15]

Training and preparedness

10.17 In response to the Committee's question on Defence's training and preparedness for radiological threats, Defence advised the Committee that 'ADF personnel undertake familiarisation training in the areas of CBRN defence as part of Basic Training' and 'some ADF groups undertake additional training based on their primary role and likely tasks'.[16]

10.18 Defence told the Committee that there are CBRN Defence Advisors in the ADF at unit level, who qualify through the School of Military Engineering's CBRN Instructor/Adviser course. These advisors receive four days of training (per course) on radiological issues.[17]

10.19 Further 'selected officers' attend an Advanced CBRN course in Canada, qualifying them to provide 'radiological threat advice to operational planning and higher headquarters'. In addition, there is a Defence Ionising Radiation Safety Officers Course for 'specialist personnel from across Defence'.[18]

Equipment, training and exercises

10.20 In response to the Committee's question on ADF units being routinely equipped, trained and exercised for radiological threats, Defence advised the Committee that this function is largely served through a specialised regiment, the Incident Response Regiment, which:

> …is prepared to deal with CBRN threats and its collective training levels are considered high. Specialist equipment and training enable its personnel to deal with radiological threats. The need for

15 Department of Defence, *Submission no.2*, p.3.
16 Department of Defence, *Submission no.2*, p.3.
17 Department of Defence, *Submission no.2*, p.3.
18 Department of Defence, *Submission no.2*, p.3.

> specific training and exercising for a response to a radiological threat scenario is determined by the assessed threat. Unit CBRN Defence Advisers provide the ability for Defence to surge its training if dictated by an increased threat.[19]

10.21 As noted, the Committee expressed interest in other agencies or services that would be involved in the event of a radiological threat, and whether Defence conducts regular exercises with these agencies.

10.22 In response, Defence advised the Committee that relevant agencies in this context were Emergency Management Australia in the Attorney-General's Department and the Australian Nuclear Science and Technology Organisation.[20]

10.23 Defence noted that the 'duties and responsibilities of these organisations are articulated in the National Counter Terrorism Handbook', produced by the Attorney-General's Department, which 'is not a publicly available document'.[21]

10.24 Defence also advised the Committee that it had created a new function within the ADF to provide support for cooperation between Defence and other government agencies on these matters:

> Defence has raised the CBRN Directorate in the Vice Chief of the Defence Force Group that, among other things, is tasked to provide a conduit for working-level engagement between Defence, Commonwealth and State Governments on CBRN matters.[22]

10.25 Defence advised the Committee that this Directorate also participates in and conducts exercises on radiological threat scenarios. At time of hearings, it was to coordinate 'Defence participation in the upcoming Department of Foreign Affairs and Trade led Discussion Exercise 'Blue Glow'. In addition, the 'Incident Response Regiment conducts regular exercises with the other agencies and organisations'.[23]

19 Department of Defence, *Submission no.2*, p.3.
20 Department of Defence, *Submission no.2*, p.3.
21 Department of Defence, *Submission no.2*, p.3.
22 Department of Defence, *Submission no.2*, p.3.
23 Department of Defence, *Submission no.2*, p.3.

Actual incidents

10.26 In response to the Committee's inquiry on whether Defence had been called upon to respond to actual radiological threats or incidents, Defence advised the Committee that:

> There is no recent history of an actual radiological threat response involving the ADF. On two separate occasions in the 1980s and one incident in 2001, Defence was requested to provide assistance to the Australian Nuclear Science and Technology Organisation in the unlikely event that damaged weather satellites entered the atmosphere and crashed into Australia. The satellites self-destructed as planned and Defence assistance was not required.[24]

Cyber warfare

Introduction

10.27 The Committee asked Defence to advise it on:

- Defence's involvement with Cyber Warfare, including which areas of activity is it pursuing, and which receive high priority;
- Measures taken by Defence to prevent unauthorised intrusions into Defence computer networks, such have occurred in other countries;
- Protections for Defence's Network-Centric Warfare (NCW) capability against such intrusions; and
- The adequacy of resources devoted to securing Australia's defence capability in this regard.

Level of involvement

10.28 In relation to its involvement in protection against cyber warfare, Defence told the Committee that all 'Internet-connected systems are potential targets for electronic attack so it is critical that Australia has an effective defensive capability'.[25]

24 Department of Defence, *Submission no.2*, p.4.

25 Department of Defence, *Submission no.2*, p.9.

10.29 Responsibility for Defence's activities in this area lies with two components of Defence:

> The Chief Information Officer Group (CIOG) in the Department of Defence employs a wide range of measures to protect its networks from such threats and actively monitors its systems to detect potentially malicious activity. The Defence Network Operations Centre provides this capability and works closely with the Defence Signals Directorate (DSD) to ensure its measures are able to protect Defence information and systems in a dynamic threat environment.[26]

10.30 Further, Defence advised the Committee that:

> DSD is pursuing areas of activity that will enhance its ability to discover and respond to threats to Government networks as well as improve our ability to identify vulnerabilities in those networks.[27]

Defence network security

10.31 Defence advised the Committee that while 'Defence does not comment on the security status of Defence information systems', the 'CIOG [Chief Information Officer Group] actively defends its systems from a range of cyber threats'.[28]

10.32 Defence told the Committee that the DSD also plays an active role in this area:

> As the national authority on information security, DSD provides material, advice and assistance to Commonwealth and State/Territory authorities. This includes assisting the Defence CIOG with cyber threat detection and warning for Defence information systems.[29]

10.33 Defence advised the Committee that both of these areas maintain close working relationships with cognate agencies:

> DSD and CIOG have ties with close allies, and cooperate with relevant agencies. When such threats have arisen in our partners' countries, DSD and CIOG have been informed and DSD has

26 Department of Defence, *Submission no.2*, p.9.
27 Department of Defence, *Submission no.2*, p.9.
28 Department of Defence, *Submission no.2*, p.9.
29 Department of Defence, *Submission no.2*, p.9.

> provided technical advice and assistance to the CIOG to ensure the confidentiality of sensitive information and the integrity of its networks.[30]

10.34 Defence advised the Committee that on a day-to-day basis:

> DSD also performs detection and reporting on cyber threats to Government agencies; this includes a seven-day, 24-hour incident response capability.[31]

Protection for Network-Centric Warfare capability

10.35 Defence advised the Committee that implementation of 'the Network Centric Warfare concept in Defence and the ADF is a critical force multiplier and it is important that the systems that contribute to that goal are protected from all forms of attack'.[32]

10.36 As a result, Defence told the Committee:

> The targets of hostile cyber warfare activities of concern to Network Centric Warfare are the networks that carry the essential information and intelligence. The protection of these networks includes physical, personnel and information security measures in accordance with Government information security.[33]

Adequacy of resources

10.37 In relation to the adequacy of resources for protection against cyber warfare threats, Defence advised the Committee that:

> The Defence CIOG operates the Defence Network Operations Centre to provide comprehensive monitoring and response to cyber threats. It assigns resources in this area commensurate with the level of threat and the sensitivity of the information being protected. Like all Government agencies, Defence CIOG benefits from DSD material, advice and assistance to protect its information systems.[34]

---

30 Department of Defence, *Submission no.2*, p.9.
31 Department of Defence, *Submission no.2*, p.9.
32 Department of Defence, *Submission no.2*, p.9.
33 Department of Defence, *Submission no.2*, p.9.
34 Department of Defence, *Submission no.2*, p.10.

10.38 Moreover, Defence told the Committee:

> DSD has received funds to enhance its cyber defence capabilities under the E-Security National Agenda, approved in two tranches by the Government in 2001 and 2006. These enhancements focus on trialling a network monitoring capability, conducting vulnerability assessments and improving training and awareness of cyber threats and security measures across government.[35]

The Hon Arch Bevis MP
Chair Defence Sub-Committee
October 2009

35 Department of Defence, *Submission no.2*, p.10.