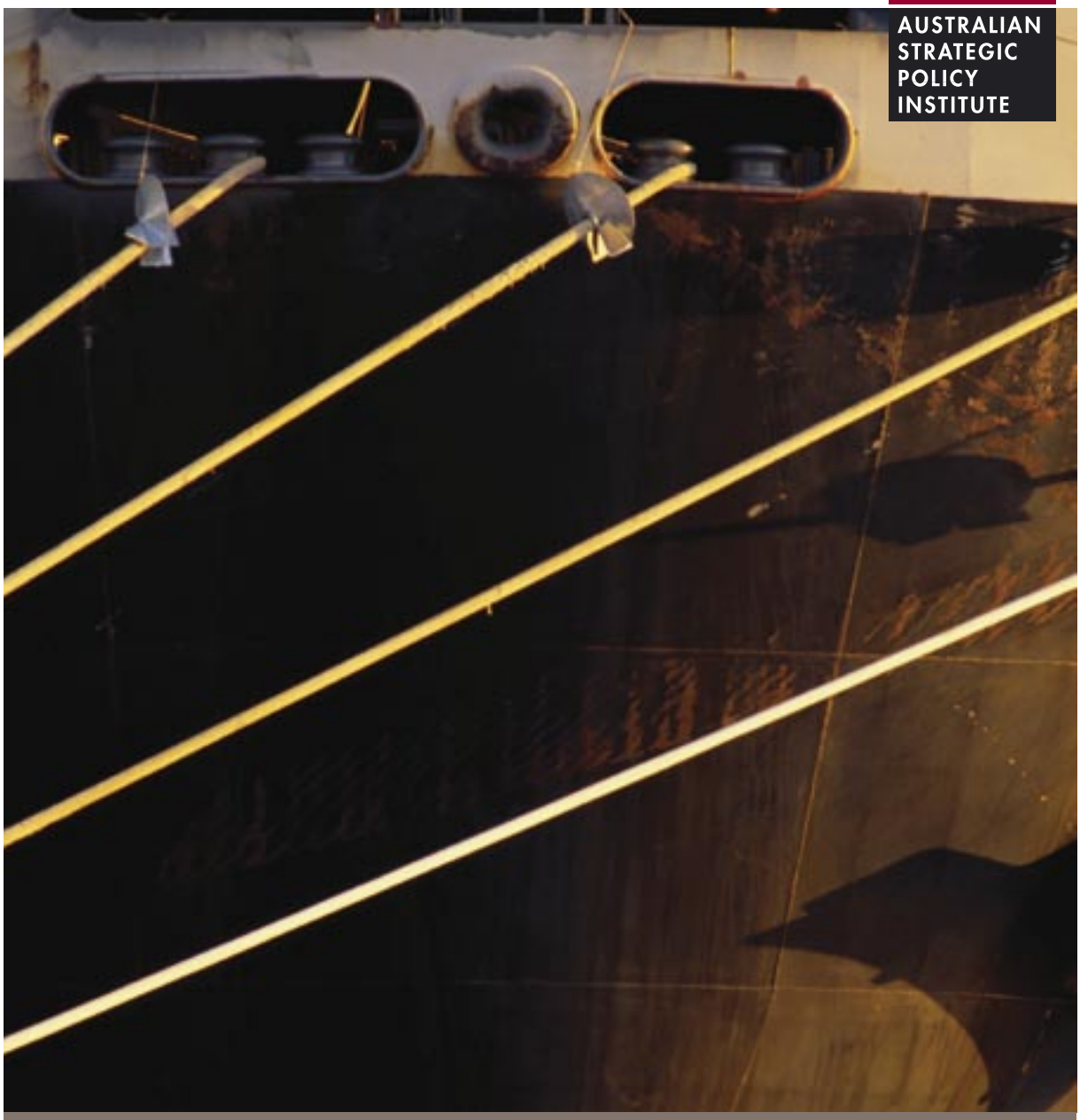
STRATEGY

ASPI

Future unknown:

The terrorist threat to Australian maritime security

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE



April 2005

Anthony Bergin

Dr Bergin is Associate Professor of Politics, University of New South Wales at the Australian Defence Force Academy in Canberra. From 1981–1985 he taught political science at the Royal Australian Naval College. From 1991–2003 he was the Director of the Australian Defence Studies Centre (ADSC). He is a member of the Australian Committee on Security Cooperation in the Asia Pacific and the Returned Services League National Defence Committee. In 2004 he introduced the first graduate subject on Australian homeland security to be taught at an Australian university.

He is the author and editor of a number of important works, including Naval Power in the Pacific (Westview, 1993), and The Pacific Patrol Boat Project—a Case Study in Defence Cooperation (ANU, 1994). He has written over 150 papers and book chapters on a wide range of national security and ocean policy issues and authored or co-authored eight major government reports in the area of marine affairs and national security. His study on the Proliferation Security Initiative will be published later this year. Dr Bergin has served as a consultant to a range of public and private sector clients.

Sam Bateman

Dr Sam Bateman retired from full-time service in the Royal Australian Navy with the rank of Commodore (one-star) in 1993 and became the first Director of the Centre for Maritime Policy at the University of Wollongong in New South Wales where he is now a Professorial Research Fellow. His naval service as a surface warfare officer included four ship commands (including a frigate and a destroyer), five years in Papua New Guinea and several postings in the force development and strategic policy areas of the Department of Defence in Canberra. His current research interests include regional maritime security, the strategic and political implications of the Law of the Sea, and maritime cooperation and confidence-building.

During 2002, Sam Bateman held a fellowship at the East-West Center in Honolulu to research developments with coast guards in the Asia-Pacific region. He is now a Co-Chair of the Council for Security Cooperation in Asia Pacific (CSCAP) Study Group on Capacity Building for Maritime Security Cooperation, and a Senior Fellow and Adviser to the Maritime Security Program at the Institute of Defence and Strategic Studies (IDSS) in Singapore.

About ASPI

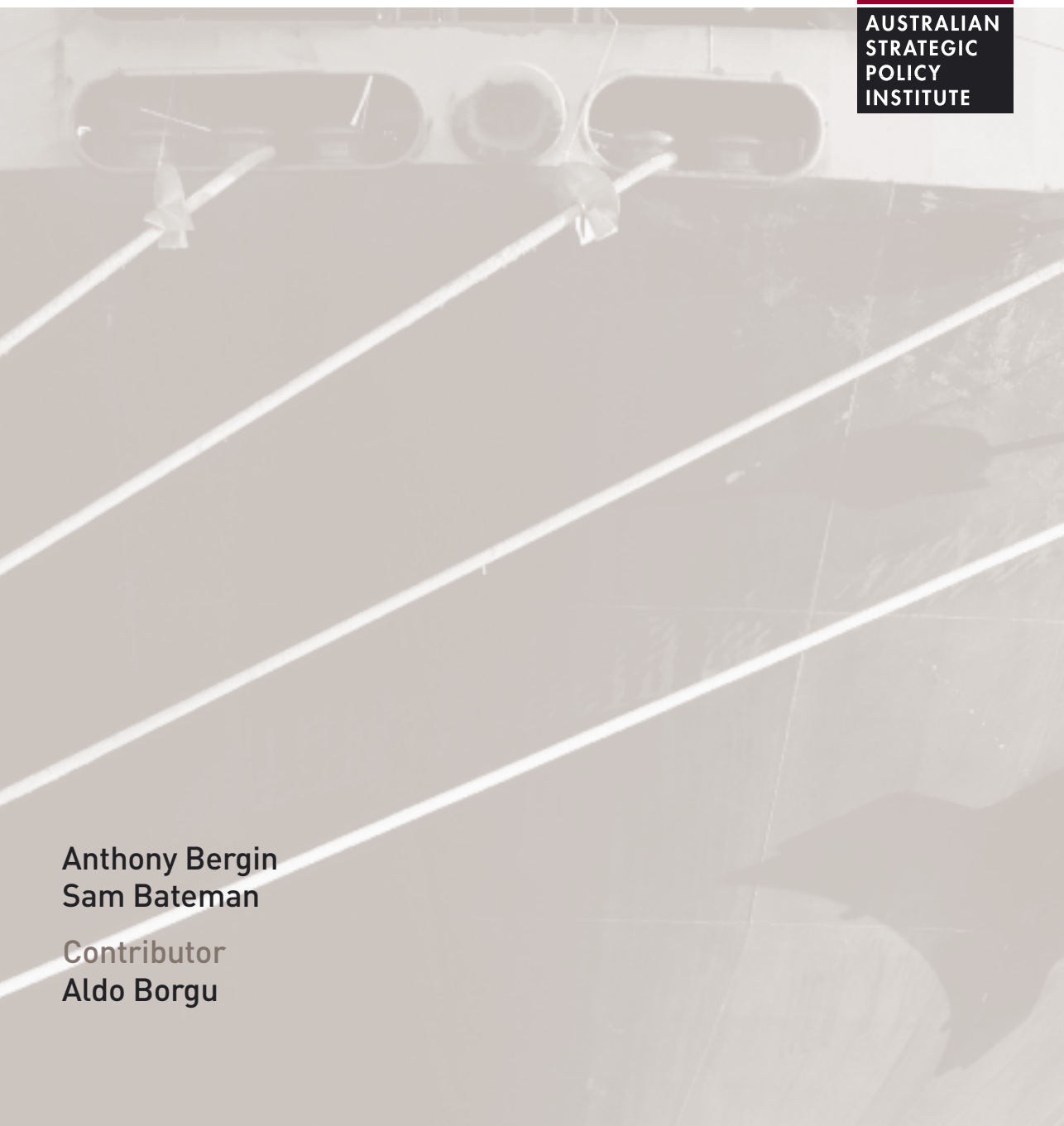
ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government.

The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Mooring lines. © APL/Corbis Westlight

Future unknown:

The terrorist threat to Australian maritime security



Anthony Bergin
Sam Bateman

Contributor
Aldo Borgu

First published April 2005

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2, Arts House
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au

Bergin, Anthony, 1954– .
Future unknown: The terrorist threat to Australian maritime security.

ISBN 1 920722 59 9.

1. National security—Australia. 2. Coast defenses—Australia. 3. Terrorism—Australia—Prevention.
I. Bateman, W. S. G. (Walter Samuel Grono), 1938– . II. Australian Strategic Policy Institute. III. Title.

355.0330994

Contents

Director's introduction

Australia's perception of the threat of maritime terrorism has been shaped by a combination of recent events, terrorist objectives and basic geography. The attacks of 9/11 and Bali underlined the general and increased threat of terrorism we now face. The attacks on the *USS Cole* and *MV Limburg* over the past five years highlighted the possibilities and dangers that maritime terrorism present.

The tendency of terrorists to attack transport infrastructure in general, while so far focussed on air, road and rail, has given rise to view the maritime sector as the next logical choice. The stated aim of al-Qaeda to focus attacks on undermining economies coupled with the dependence of those economies on maritime trade and current terrorist attacks on the energy industry in particular, such as on-shore and off-shore oil refineries and pipelines in Iraq and Saudi Arabia heightens the threat further.

Finally the geography of our immediate neighbourhood, maritime Southeast Asia, and the presence of numerous choke-points in that region as well as Australia's own peculiar geography, its large coastline, small population base, offshore resources, and dependence on overseas trade makes us particularly vulnerable to such attacks.

Of course such attacks are not inevitable. Indeed one important question that needs to be asked—and answered—is why we haven't witnessed a greater number of maritime terrorist attacks to date. However a terrorist attack on Australia's maritime interests remains a credible scenario. Past experience alone tells us we can't afford to rely on a terrorist group's past actions as a guide to its future attacks.

The government has directed and overseen major developments in enhancing Australia's maritime security at some considerable cost to taxpayers and industry. But more needs to be done. This report identifies where gaps exist in current policies and arrangements and the result is a series of recommendations including ways to improve

Photo opposite: Tanker and mooring lines. © APL

coordination between federal and state agencies and the need to provide additional resources.

Any report that deals with the modern threat of terrorism by necessity covers many responsibilities and jurisdictions, not least three levels of government, the private sector and groups within those areas. This report is no different and it couldn't have been prepared without the active cooperation of many individuals and organisations within Australia's maritime sector. To them I extend my thanks for devoting their time and ideas, especially through their attendance at a round table held in Canberra to discuss earlier drafts of the report.

Thanks go to Dr Anthony Bergin and Dr Sam Bateman who wrote the report as well as Aldo Borgu who managed the project overall and contributed to the section dealing with the threat of maritime terrorism.

As always the views expressed in this report are those of the authors, they do not reflect the views of ASPI as an institution. Peter Jennings, ASPI's Director of Programs is responsible for the publication of the document.

Peter Abigail
Director

Executive summary

The threat of maritime terrorism has led to fundamental changes in the international maritime security environment. There have been major developments in the regulation of international shipping, particularly through the introduction of the International Ship and Port Facility Security code. The Australian Government moved quickly to implement the code in Australia through the *Maritime Transport Security Act 2003* (MTSA), and to introduce a range of other maritime security measures, including additional facilities for screening containers and tighter immigration controls at seaports. The new measures have imposed large additional costs on the transport system and involved significant effort from both government and industry.

Aviation and maritime security pose very different challenges. There's a relatively high level of aviation awareness in Australia, but this isn't so with maritime awareness. While airports are basically similar, every seaport is different. The security of ports and ships must consider all environments: land, air, sea surface and subsurface. Most importantly, however, their security involves a fundamental division of responsibility between the Commonwealth, the states and territories.

A terrorist attack on Australia's maritime interests is a credible scenario. We have high dependence on shipping and seaborne trade, and are adjacent to a region where terrorist groups have maritime capabilities. Major terrorist threats include:

- a direct attack on a port facility (especially a container, oil, gas or chemical terminal)
- a direct attack on a ship, particularly a high-risk vessel, such as one carrying high-consequence dangerous goods, a passenger ferry, a cruise liner, or a US Navy vessel in an Australian port
- an attack on a ship, to hijack it and use it as a weapon against something else
- the use of a ship, its cargo or a sea container for terrorist purposes to transport terrorists or terrorist material, including a possible weapon of mass destruction.

Keeping the broad expanse of our maritime approaches secure is extremely difficult. The new Joint Offshore Protection Command and the Maritime Information System, announced by the government in December 2004, will be a marked improvement. However, a determined and expert terrorist is still likely to have little difficulty in entering Australia by sea, and will probably only be defeated by advance intelligence of his movements.

Australia faces major challenges in reducing the risks of maritime terrorism. These are institutional (to ensure coordination between the national and state/territory agencies involved with maritime security) and operational (to meet the demands of geography and distance). We haven't met these challenges fully, and we lack consistency in the response across the states and territories.

This report identifies where gaps exist in current arrangements. It includes recommendations to improve coordination between national and state agencies and to develop the national capacity to manage maritime security in the longer term. Other problem areas include the management of high-consequence dangerous goods, the management of the supply chain, and possible risks associated with the employment of large numbers of foreign seafarers on the Australian coast.

The report draws a distinction between the *protection* of ships, ports and port facilities, which requires a range of physical and personnel security measures (basically to conform with the MTSA), and *prevention and response*, which requires effective operational measures to prevent attacks and respond to actual threats. The costs of the former are those of doing business and are legitimately borne by the owner or operator, but the costs of the latter should be met by government. We need greater transparency of risk determination and cost allocation to avoid excessive burdens being placed on industry and state governments.

Although the Federal Government has dramatically increased spending on counter-terrorism measures, so far few, if any, additional resources have been provided for the prevention and response elements of maritime security in ports or close to shore. Several recommendations are made to redress this situation, including the establishment of a Maritime and Port Security Program, the strengthening of state water police, the establishment of state port police, and a specific role for the Australian Defence Force in ship and port security.

Recommendations

Legal and jurisdictional

1. The state premiers and the Northern Territory Chief Minister should meet jointly to consider jurisdictional, legal, information-sharing and resource issues related to the coordination of capabilities to provide maritime security, including how the Joint Offshore Protection Command will interact with them in preventing and responding to maritime security threats or attacks.

Protection

2. The states should establish dedicated port police units for major ports to work with state water police, and be responsible for port security on the landside.

3. The Australian Government should introduce a $100-million Maritime and Port Security Program over three years, on a cost-shared basis, to further modernise and strengthen maritime and port security systems and programs.

4. To strengthen container security, Australia should adopt the US 24-hour manifest rule for cargo destined for Australia and monitor developments in container seal and tracking technologies. Customs should also randomly inspect transshipped empty containers.

5. The Department of Transport and Regional Services (DOTARS) should be given a clear mandate to secure the entire supply chain and work with Customs, the Department of Foreign Affairs and Trade (DFAT) and the Critical Infrastructure Protection Branch of the Attorney-General's Department to adopt a broader supply-chain security perspective that ensures port, ship and cargo security.

6. The Australian Government, through the Office of Transport Security (OTS), should develop publicly available guidelines for the security of high-risk ships in Australian ports, including for port visits by US Navy vessels.

7. The Australian Government should conduct an investigation of the risks involved in the employment of large numbers of foreign seafarers on the Australian coast, including on vessels carrying high-consequence dangerous cargoes.

Prevention and response

8. The states and the Northern Territory should strengthen security at major ports by upgrading their on-water capabilities.

9. The Australian Defence Force should have a direct involvement in providing security for ships, ports and port facilities against the threat of maritime terrorism. This responsibility should be assigned to the appropriate operational commander and include the establishment of Mobile Maritime Security Response Teams.

10. The Joint Offshore Protection Command should give the highest priority to the development of effective maritime domain awareness, using all sources of relevant information.

11. The government's campaign to raise public awareness about the risks of terrorism should include information to the community, especially the maritime community, on the risks of maritime terrorism.

Cooperation and capacity building

12. State governments should establish state maritime security committees to develop, coordinate and integrate processes at security-regulated and other ports. The state committees would be the key components of a national maritime security architecture that links to the national-level Maritime Industry Security Consultative Forum.

13. The Australian Government should commission a comprehensive analytical study to identify key vulnerabilities of ports, port facilities and shipping.

14. The Australian Government should take action to reverse the current trend towards a declining maritime skills base, including through a sponsored cadet scheme to encourage young men and women to pursue a career at sea, and a review of the taxation regime for Australian seafarers working overseas.

15. The Protective Security Coordination Centre, in cooperation with state police, port authorities and DOTARS, should initiate a regular round of confidential workshops for developing port security responses and maritime exercises to test port security leaders.

16. Australia's Chief Scientist should prepare a paper that addresses the scientific, technological and analytical requirements for Australian port and maritime security.

17. The work of the inter-departmental committee on regional maritime security cooperation should be given high priority and sufficient funding provided to implement its proposals.

Draft state premiers' statement on maritime security

The state premiers and the Chief Minister of the Northern Territory appreciate the need for a consistent and coordinated national approach to dealing with the maritime terrorist threat. In doing so, they:

- welcome the lead being provided by the Australian Government on maritime security
- note that state and territory interests in transport security and public safety tend to be broader than the Commonwealth interest in those aspects of port and shipping security that come under *Maritime Transport Security Act 2003* (MTSA)
- acknowledge the advantages of establishing a more consistent and coordinated approach across the states and territories, as well as within those jurisdictions

but

- stress the importance of respecting the existing division of maritime jurisdiction between the Commonwealth and the states, as set out in the Offshore Constitutional Settlement.

Threats

A consistent, nationwide approach is required to managing the security of high-risk ships, including those carrying high-consequence dangerous goods. The Australian Government should take a leading role in this by developing guidelines for the security of such ships while they're alongside or moving around in a port. The guidelines need to recognise that adequate security will be best provided by appropriately armed and trained military or police personnel.

Legal frameworks

The interaction between state or territory legislation, and Commonwealth powers and responsibilities under the MTSA, the Customs Act, the Defence Act and other relevant Commonwealth

legislation is complex. The states and the Northern Territory will investigate the need for complementary legislation to apply MTSA-type provisions to vessels and facilities under state or territory jurisdiction that are not currently regulated under the MTSA.

Institutional arrangements

The Joint Offshore Protection Command is a welcome initiative by the Australian Government, but we need to understand how the new command interacts with state jurisdiction over emergency services, police, directors of public prosecutions and coroners in the event of a maritime security incident.

The establishment of state and territory maritime security committees would help overcome current problems of coordination, information-sharing and communications. The committees should include representatives of state counter-terrorism bodies, major port authorities, police (including water and transit police), emergency services, maritime safety agencies, state transport and logistics agencies, and state-based representatives of such national agencies as the Office of Transport Security, the Australian Customs Service, the Australian Quarantine and Inspection Service, the Australian Secret Intelligence Organisation and the Royal Australian Navy.

Resources

The states and the Northern Territory have a range of capabilities that can potentially assist in providing surveillance and enforcement support for national maritime security. These include patrol craft and surveillance systems operated by fisheries services, marine safety agencies and environmental protection agencies, as well as state water police.

The possibility of dedicated port police units for major ports, to work with state water police and be responsible for port security on the landside, will be investigated.

The need to strengthen maritime security by upgrading the on-water strength of state and Northern Territory agencies is acknowledged. This might be achieved by making the water police more capable and/or by rationalising other state marine surveillance and enforcement capabilities.

Funding

Australia's security against the threat of maritime terrorism must be strengthened. We, the State & NT Governments acknowledge the extensive Federal investment in strengthening Australia's counter-terrorism arrangements. The States and the NT are also committed to providing an appropriate level of funding to further enhance port and maritime counter-terrorism measures.

A number of new measures identified in this statement will put even greater pressure on state budgets. We ask the Commonwealth to further consider appropriate financial burden-sharing that recognises the importance of measures to counter maritime terrorism.

A distinction must be drawn between the costs of the physical measures to protect a ship, a port or a port facility to implement ISPS Code requirements, and those of the operational measures needed to prevent or respond to an actual maritime terrorist threat or attack.

The former are the costs of doing business and should be carried by the owner or operator of the ship or port facility. The latter display the attributes of a *public good*, as their objective is to protect the community from a disaster rather than to protect a ship or port facility. These costs should be met by government, and we need to discuss with the Prime Minister how this burden might be shared between the different levels of government.

Chapter 1

THE NEW MARITIME SECURITY ENVIRONMENT

Introduction

About 90% of the world's trade volume moves by sea, and this volume may double over the next fifteen years. About 99.5% of Australia's overseas trade by volume, and 75% by value, is carried by sea. Seaborne trade is potentially vulnerable to terrorist attack because of the quantity of cargo involved, the trade's diverse and large international labour force, the difficulties of enforcement in port and at sea, and the poor regulatory environment of international shipping—which includes low levels of accountability, complicated chains of ownership and a high incidence of fraudulent documentation.

International shipping

Here is a sector characterised by an extremely diverse international labour force, transporting a vast range of goods whose provenance, description and ownership are often left remarkably vague. This is a system where international transport chains involved thousands of intermediaries, on vessels registered in dozens of countries that sometimes choose not to uphold their international responsibilities and where some vessel owners can and do easily hide their true identities using a complex web of international corporate registration practices.

Security in Maritime Transport: Risk Factors and Economic Impact, OECD, July 2003, p 5

Photo opposite: Rope and cleat. © APL

The need to counter the threat of maritime terrorism has led to fundamental changes in the international maritime security environment and in the maritime strategies of most countries, especially major sea-trading nations such as Australia. The required countermeasures impose large additional costs on the transport system and involve significant effort from both government and industry. However, at this stage, the maritime terrorist threat has had no significant impact on the volume or pattern of international trade. Stronger than expected Asian economic growth has been unaffected by various terror attacks.

The maritime terrorist threats within the scope of this report include:

- an attack on an Australian port facility, the international supply chain, a ship or ships in an Australian port or at sea off the Australian coast, a ship carrying cargo from or to an Australian port, an Australian-flag vessel or warship overseas, or an offshore oil and gas installation, undersea cable or pipeline in Australian waters
- the use of the maritime transportation system or a vessel to bring terrorists or their materials—in the worst case scenario, a weapon of mass destruction (WMD)—into Australia for terrorist purposes.

The threat of maritime terrorism

Definitions

For the purposes of this report, we define maritime terrorism as the use of violence against a ship, its passengers, cargo or crew, a port facility or fixed or floating platform for political ends. This includes any use of violence for the purpose of putting the public or any section of it in fear, with the intention of directly or indirectly influencing a government. Our definition also encompasses the use of the maritime transportation system to introduce terrorists or terrorist materials into Australia.

The Commonwealth *Criminal Code Act 1995* states that a terrorist act is an action or threat of action that causes certain defined forms of harm or interference, and the action is done or the threat is made with the intention of advancing a political, religious or ideological cause. The forms of harm include serious physical harm to a person, serious damage to property, a person's death, and serious interference to an electronic system, including telecommunications and information systems.

Incidents

The July 2004 White Paper *Transnational Terrorism: the Threat to Australia* (Australian Government 2004) identified twenty-six major attacks linked to transnational extremist-Muslim terrorism since 1992. Only four of these might be considered maritime related. These were the attacks on the USS *Cole* in Aden in October 2000, the French tanker *Limburg* off Yemen in October 2002, the oil refinery in Yanbu, Saudi Arabia, in May 2004 and on the Al-Khobar Petroleum Centre, Saudi Arabia also in May 2004.

By focusing only on extremist-Muslim attacks, the White Paper excluded the many maritime terrorist attacks by the 'Sea Tigers' of the Liberation Tigers of Tamil Eelam on merchant ships and Sri Lankan warships. More significantly, the White Paper omitted the most serious maritime terrorist attack by an extremist Muslim group—the attack by Abu Sayyaf terrorists on the Philippine passenger ferry *Superferry 14* in February 2004 (see box). By its nature and its nearness to Australia, the Abu Sayyaf attack possibly provides the best model of a credible threat in Australian waters.

Superferry 14

- Attack occurred on 27 February 2004.
- A bomb exploded and the ship caught fire ninety minutes after leaving Manila, with 899 passengers and crew on board.
- Sixty-three people were killed and fifty-three others were missing, presumed dead.
- The combined toll of 116 made this the worst known terrorist attack in the Philippines.
- The Abu Sayyaf group claimed responsibility, but this was initially denied by the Philippine Government
- Six militants linked to al-Qaeda were charged with the bombing in October 2004.
- The bomb was left in the engine room, but was allegedly carried on board in a TV set as passenger baggage.
- The perpetrator(s) then left the ferry before it sailed.

A Philippines Coast Guard helicopter pours water into the burning passenger ship Superferry 14 following a terrorist bombing, February 2004. EPA via AAP © 2004 EPA

The main maritime terrorist threat to Australia's shipping and ports is posed by al-Qaeda and its associated groups in Southeast Asia, particularly Jemaah Islamiyah (JI). JI has training camps in the southern Philippines, and its members routinely move between Sabah, Indonesian Borneo and these camps by speedboat, local craft and ferries. The Abu Sayyaf group in the Philippines has already shown that it can attack ships underway. Threats have been made to attack US naval ships and facilities in Singapore. As recently as March this year Philippine military sources were quoted in the media as saying that Abu Sayyaf was training with JI to prepare for possible seaborne and underwater attacks outside the Philippines.

The main maritime terrorist threat to Australia's shipping and ports is posed by al-Qaeda and its associated groups in Southeast Asia, particularly Jemaah Islamiyah (JI).

Terrorism has more sophisticated aims than just killing people. Al-Qaeda has stated that it might attack vital economic centres and strategic enterprises of the 'Jewish–Christian alliance', including operations on land, at sea and in the air. Australia has been mentioned in statements attributed to al-Qaeda.

The government's threat assessment

On 30 April 2004, the Australian Government released to relevant national and state/territory agencies an Australian Security Intelligence Organisation (ASIO) assessment of the threat to Australia's shipping and port infrastructure from terrorism. The publicly released version of the assessment contains few details, but makes the following statements.

- Al-Qaeda and its associated groups in the region have a stated intention to attack Australian interests and are known to have a capacity to conduct significant terrorist attacks, including against maritime interests.
- ASIO's assessment is that al-Qaeda's capacity for terrorist attacks continues to develop, but that the group's previous actions aren't necessarily a guide to future activity, and that protective security policy and planners should work on the basis of preparing for the unexpected.
- ASIO has concluded that the threat to many aspects of Australia's shipping and port facilities is low or very low, although there are some areas (not identified) that have been assessed as a medium threat.
- Intelligence is being made available to government and the maritime industry where information is needed to ensure that effective and appropriate protective security measures are in place.

These views were echoed in the government's July 2004 White Paper, which stated that 'transnational terrorists have demonstrated maritime attack capability.' Citing the USS *Cole* and MV *Limburg* cases, the paper went on to state that 'further attacks have been planned but disrupted' and that 'most attacks occur (or are planned) in coastal waters.' The attractiveness to terrorists of maritime targets within Australia was also highlighted by the arrest of al-Qaeda suspect Willy Brigitte. The targets he was apparently scouting included the naval dockyard at Garden Island in the heart of Sydney.

In any event, while such government assessments state that al-Qaeda and associated groups continue to have a *capacity* to carry out terrorist attacks against maritime interests, the assessments don't say, at least publicly, whether those groups have such an *intent* (see box). This might be why the threats are assessed as ranging from low or very low to medium. Also of some interest is the fact that JI and its maritime capabilities were not mentioned specifically in the threat assessment, although it may be argued that this was because JI fell into the category of al-Qaeda's 'associated groups in the region'.

The Australian Government's maritime threat assessment needs to be judged not only from its statements but also from its actions. The government's decision in November 2003 to lay up two of the Navy's recently delivered minesweepers suggests that the government doesn't believe that terrorists will have the capability to lay mines in our immediate region any time soon. It's expected that it would take at least six to twelve months to bring these ships back into operational service.

Why haven't we seen more maritime terrorism?

Terrorists don't always live up to either their own potential or our worst fears. One question worthy of further analysis is why groups such as al-Qaeda and JI haven't engaged in more maritime terrorist attacks. Assuming that they actually have the capability for maritime attacks, the reasons they haven't done so might include the following:

- Attacking maritime trade doesn't offer the same prospects for casualties as attacks on land. When people think of 9/11 they don't think about the billions of dollars wiped from the US economy, but of the twin towers tumbling and 3,000 dead. However, this still doesn't explain why maritime mass transport infrastructure such as ferries hasn't been targeted more.
- Terrorists may only look to maritime terrorism once our counter-terrorist policies make other operating environments too difficult. We shouldn't underestimate the degree to which counter-terrorist measures to date have made the maritime operating environment more difficult.
- If we accept that terrorists, for the most part, are rational actors, then any act that threatens the global economy (such as closing a port or restricting trade) would invite a disproportionate and united response that might threaten their existence in the longer term.
- Media reports identifying a fairly substantial investment by al-Qaeda in the shipping industry may signify that the maritime sector is more useful as a means of transportation and fundraising. For the time being, al-Qaeda may not be willing to jeopardise this.
- Terrorist groups may still be at an early stage of developing their maritime attack capabilities. We shouldn't underestimate the difficulty of planning and mounting a sophisticated maritime attack—after all, that's why such capabilities are the domain of the Special Forces of nation states.
- The background and training of key terrorists also has an impact. One of the reasons the Sri Lankan Tamil Tigers have the most sophisticated maritime terrorist capability in the world is that a number of their senior leaders were fishermen by trade. If JI begins to recruit among Indonesia's pirates, for example, the group could change its tactics towards great use of maritime attacks. That being said, the potential for future cooperation between pirates and terrorists has been overstated somewhat.
- Finally, much of terrorist targeting comes down to opportunity: nothing attracts a terrorist quite as much as the chance of success. Terrorists are usually meticulous in their planning, and strike once a vulnerability becomes apparent in a worthwhile target. They may have already chosen a maritime target, and simply be waiting for it to become vulnerable again.

Concepts of maritime security

What do we mean by 'maritime security'? Navies have their own understanding of what the term means. Their role is to protect the nation and its national maritime interests against threats from the sea and at sea. This role is in line with governments' first responsibility to provide for the security and wellbeing of their citizens, including protection of national sovereignty. The policy responses have traditionally been formulated on the basis of strategic appreciations of the security environment, especially assessments of the capabilities and intentions of potential adversaries, and of the warning time in which these capabilities and intentions might change.

This situation changed after 9/11. Maritime security is still concerned with protecting against threats from the sea and at sea, but instead of overt threats from military forces, the threats of current concern are veiled and perhaps even 'unthinkable'. A fundamentally different approach is needed for assessments of capabilities, intentions and warning time. Terrorist capabilities and intentions may simply not be known, but this shouldn't mean that we work only on the basis of 'worst case scenarios', which are prevalent in discussions of the threat from maritime terrorism. In the interests of responsible public expenditure and avoidance of unreasonable burdens on the private sector, new maritime security measures should be subject to rigorous analysis and testing against realistic and commonsense risk assessments. In this regard, new counter-terrorism measures are little different from new capability proposals within the Department of Defence.

This new focus for maritime security is apparent in the work of the International Maritime Organization (IMO), particularly through the International Ship and Port Facility Security (ISPS) Code, to make international shipping and seaborne trade more secure against the threat of maritime terrorism. This new approach doesn't accord with what navies and defence forces regard as 'maritime security'. Navies have seen their responsibility as protecting the nation beyond its shores and aren't necessarily involved with the security of port facilities or ships in port. These activities are regarded as civil policing responsibilities and the task of marine police or a coast guard.

What's the interface between the traditional concept of maritime security held by navies and the new concept evident in the ISPS Code and measures to secure shipping and seaborne trade against the threat of terrorism? Navies have always been involved in the protection of shipping and would provide the top end of response capability in the event of a terrorist attack or the threat of one. Defence forces are the 'muscle' and 'weapons of last resort' in countering terrorism.

The US tends to treat domestic and national security as separate requirements (Flynn 2004). National security is equated with protecting the nation beyond its shores—what might usually be seen as national defence—while domestic security is what takes place on land. Domestic security includes the hardening of critical infrastructure, personnel identity documentation for people working on ships and in ports, and arrangements for port security on both the land side (perimeter fencing, access controls etc) and on the water side (channel security, water borne security patrols).

Border protection is another major dimension of national security. It includes preventing the transportation system being used to import terrorist materials (including WMD) or

other illicit cargo (drugs, arms and even human beings), as well as surveillance, patrols and response at sea to protect sovereignty, to prevent illegal entry and to enforce national laws.

Safety and security

There's a close relationship between maritime safety and maritime security. In the past, it was normal in the shipping sector to distinguish between safety and security. For example, the 1974 International Convention for the Safety of Life at Sea (the SOLAS Convention) related to safety at sea, specifying minimum standards for the construction, equipment and operation of merchant ships, while the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) and its protocol covered offshore installations and related to security. However, since 9/11 the safety and security of shipping are closely linked. Indeed, the IMO has recently changed its motto from 'safer ships, cleaner oceans' to 'safe, secure and efficient shipping on clean oceans'.

In Australia, maritime security is the responsibility of the Office of Transport Security (OTS); maritime safety, including search and rescue, is the responsibility of the Australian Maritime Safety Authority. Both agencies are within the Transport portfolio, but nevertheless problems of coordination might arise. The practice of many countries is to locate the two functions within the one agency, recognising that they require similar reporting and inspection procedures.

Safety and security aren't mutually exclusive. Maritime safety is part of comprehensive security and includes maritime safety services (including search and rescue and rescue coordination centres), marine environmental protection (especially the prevention of and response to ship-sourced marine pollution), marine navigational aids and services, and ship and personnel safety services (such as marine surveys, state/territory port control, marine accident investigations, marine qualifications and identity documentation).

Maritime security is different

The nature of the attacks on the World Trade Center focused attention on aviation security. After an initial tendency to apply the principles of aviation security to maritime security, it was quickly appreciated that maritime security is different.

In Australia, most people fly and the community has a relatively high level of aviation security awareness, but this is not the case with maritime awareness. There's relatively little community understanding of the nature and complexity of the operation of ships and ports, or of their economic significance and vulnerability. A particular manifestation of this situation is the lack of a strong maritime skills base in Australia, and the looming serious shortage of people with seagoing qualifications.

The security of ports and ships must cover all environments: land, air, sea surface and subsurface. Airports have defined perimeters and usually some form of 'buffer zone' between the airport and other activities. Access is fairly easily controlled. Airline passengers expect to be screened with their baggage, and airline and airport workers can be closely monitored. In comparison, ports may not have a clearly defined perimeter, even on the land side. The public have long visited ports to watch ships or to fish. Ports might have multiple road and rail access points.

On the waterside, ports are practically impossible to secure physically. Extensive fishing and recreational boating may occur within the port precinct. Ports vary greatly in their physical attributes (see Figure 2), while airports are all basically similar—as one port official noted, 'If you've seen one port, you've seen one port'.

After an initial tendency to apply the principles of aviation security to maritime security, it was quickly appreciated that maritime security is different.

Under Australia's Offshore Constitutional Settlement, state authorities have jurisdiction out to three nautical miles from the territorial sea baseline and for internal waters, including jurisdiction over ports and port areas. The settlement's Shipping and Navigation Agreement divides jurisdiction over shipping between the Commonwealth and the states and territories. The states and the Northern Territory are responsible for trading ships on intrastate voyages, fishing vessels, pleasure craft and inland waterway vessels, and the Commonwealth has responsibility for:

- trading vessels on an interstate or international voyage
- intrastate trading vessels declared under section 8AA of the *Navigation Act 1912*
- fishing vessels and fishing-fleet support vessels on an overseas voyage
- ships belonging to the Commonwealth or a Commonwealth authority
- offshore industry mobile units and vessels, other than those confined to one state or territory.

Brisbane port. Photo courtesy Port of Brisbane Authority

This division of responsibility between the national and the state and territory governments has no parallel in aviation. The Commonwealth simply asserts jurisdiction over aviation, and most major airports are subject directly to Commonwealth legislation. While the Australian Federal Police (AFP) and AFP Protective Service provide security for major airports, security for ports is provided by state police or commercial security contractors, and there are potential difficulties with Australian Government agencies, including the Australian Defence Force (ADF), exercising powers within state jurisdictions.

Chapter 2

WHAT ARE THE RISKS IN AUSTRALIA?

Introduction

The risks of a maritime terrorist attack on Australia flow from our dependence on shipping and seaborne trade, our extensive involvement in international shipping, the location of many port facilities close to major population centres, and our reliance on offshore oil and gas to maintain energy self-sufficiency. We also live in a region where terrorist groups possess maritime capabilities, and much of our overseas seaborne trade passes through areas at risk of terrorist attack.

Meeting these risks is a challenging task. Major challenges are:

- *institutional*—ensuring appropriate coordination between the diverse Australian Government and state/territory authorities involved in maritime security
- *operational*—meeting the demands of geography and distance.

Some Australian ports and offshore oil and gas installations are located in very remote areas. Security resources will always be spread thinly, and ensuring a timely response to a terrorist threat or incident will inevitably be difficult. These factors place a premium on intelligence and surveillance to provide early warning of a threat.

Seaborne trade

The sheer magnitude of Australia's shipping task is daunting. Nearly 700 million tonnes of cargo move across Australian wharves each year. About 75% of this is international exports, 9% international imports, 8% coastal cargo loaded and 8% coastal cargo discharged.

Photo opposite: Offshore oil rig. © APL/Evan Collis

During 2002, 3,298 foreign-flag commercial ships made 18,043 separate calls at Australian ports, and around 115,000 individual foreign seamen entered Australia. By value, container ships dominate both imports and exports. Dry bulk carriers account for about 63% of total seaborne trade by volume; liquid bulk carriers transport around 10% (mainly crude oil and petroleum products).

Tankers bringing crude oil from the Middle East carry the largest volume of imports, while dry bulk carriers carry the greatest weight of exports. Our exports vastly outweigh our imports because of the types of products we ship (coal, iron ore, grain, alumina, manganese etc). Exports and imports of crude oil and petroleum products total about 50 million tonnes each year, and chemicals total about 6.4 million tonnes. Except for the Bass Strait trade, most coastal cargo is also liquid or dry bulk.

During 2002, 3,298 foreign-flag commercial ships made 18,043 separate calls at Australian ports, and around 115,000 individual foreign seamen entered Australia.

Australian merchant fleet

The Australian-owned merchant fleet has steadily decreased both in numbers and in gross tonnage over the past ten years. There were seventy-seven Australian-owned merchant vessels at 30 June 2002, of which sixty-three were Australian registered. In addition, Australian entities operate an undetermined but significant number of other vessels under time charter that aren't subject to Australian domestic maritime legislation.

This situation has both costs and benefits in maintaining security against threats of maritime terrorism. With a high proportion of Australia's seaborne trade carried by foreign vessels, Australia's maritime security is potentially weakened. Masters and officers of these vessels may lack local knowledge, and controls over foreign seamen may not be as effective as those over Australian seafarers.

Cargo already on board a foreign ship has to be reported and is subject to risk profiling. It may be inspected by Australian authorities while the ship is on the Australian coast.

Coastal voyage permits

Part VI of the Navigation Act with a few exceptions, requires vessels trading interstate to be licensed or have a permit. The Department of Transport and Regional Services (DOTARS) administers these licences and permits, which are listed on the DOTARS website. About 20% of the vessels licensed to trade interstate in August 2004 were foreign-registered vessels. An unlicensed ship may be granted a permit to trade on the Australian coast in the carriage of either cargo or passengers, where:

- there's no suitable licensed ship available for the shipping task or
- the service carried out by licensed ships is inadequate, and
- it's in the public interest that an unlicensed ship be allowed to undertake the task.

Two kinds of permits are issued:

- A *single voyage permit* (SVP) is issued for a single voyage between designated ports for the carriage of a specified cargo or passengers.
- A *continuing voyage permit* (CVP; strictly, a 'Permit to Unlicensed Ship—Continuing') is issued for a period of up to three months to enable a vessel to carry specified cargo between specified ports.

Most CVPs are issued to carry domestic cargo as part of an international voyage. The permits are issued subject to a number of conditions, including that a vessel not be detained under Australia's Port State Control program. There's no specific condition relating to security requirements.

Vessels are licensed to participate in Australia's coastal trade irrespective of flag or crew, but the vessel must not be in receipt of a subsidy from a foreign government. The crew must be paid Australian wages while trading on the Australian coast.

In 2001–02, 997 voyages along the Australian coast by foreign-flag ships used voyage permits (647 SVPs and 350 CVPs). Voyage permits for the iron ore and petroleum industries have increased.

Although foreign-flag vessels entering Australia will meet international security requirements (see Chapter 3), the level of confidence in the security checking of their crews will be lower than for Australian-flagged vessels. The system depends on the accuracy of the crew list supplied by the ship, and it may be difficult to detect fraudulent documentation. Unlike most other visitors to Australia, ship crew members (like aircrew) don't apply for a visa in advance. On arrival in an Australian port, they're granted a 'special purpose visa' provided they hold both a valid national passport and a seafarer's identity document. One hundred and thirteen foreign seafarers 'jumped ship' in Australia between July 2001 and April 2004.

The weakest link?

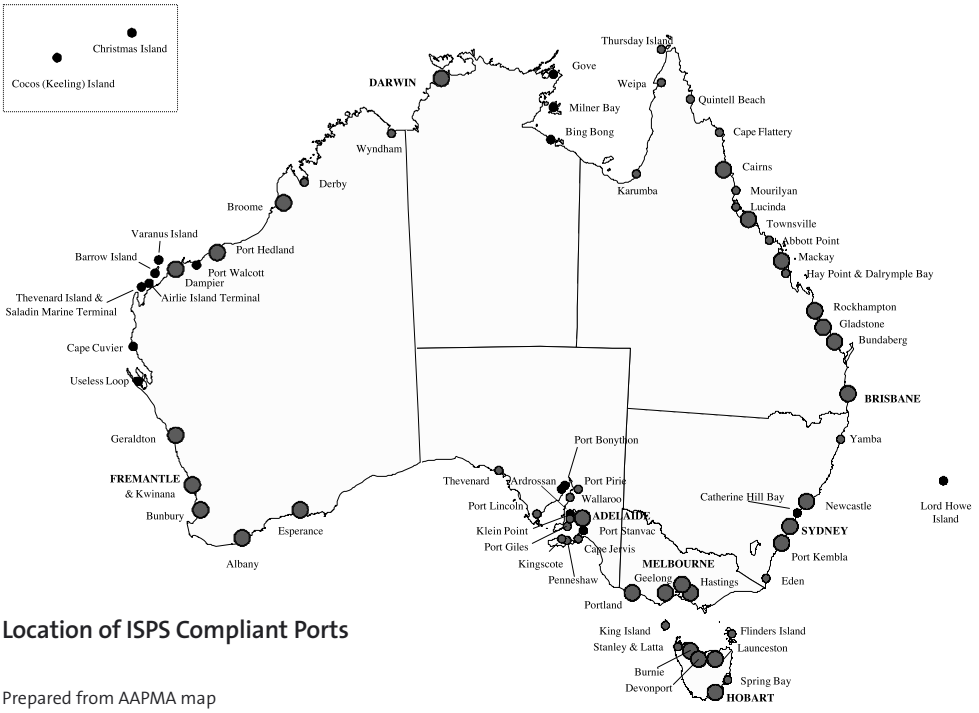
International shipping is arguably the weakest link in our national security system. Foreign flag vessels from all over the world enter Australian waters daily. Onboard are both people and cargoes that represent a potential risk to Australians.

Independent Review of Australian Shipping, September 2003, para 130

Ports

There are approximately seventy commercial ports around Australia's 37,000-kilometre coastline (see Figure 1), sixty of which regularly handle international passengers or freight. Over 300 separate port facilities are located within these ports. Some of these facilities handle chemicals and other materials that are extremely flammable, toxic or both.

Figure 1: Location of security-regulated ports



Location of ISPS Compliant Ports

Prepared from AAPMA map

Reflecting the nature of early European settlement in Australia, Australia's major ports are mostly within parent cities. With the exception of the port of Brisbane, which has been able to expand through reclamation works at the mouth of the Brisbane River, major ports and their facilities are often tightly confined by residential or other industrial areas and are the foci of heavily congested road, rail and waterway routes. They're gateway ports, rather than transshipment centres. By world standards, they deal with medium volumes of cargo. Melbourne, our largest container port, handles around 1.5 million containers each year. By contrast, Singapore handles 17 million and Rotterdam handles 7 million.

Most major Australian port authorities are owned by state governments, and are structured as corporations. Other, private ports handling general cargo, minerals and petroleum include Geelong, Portland, Gove, Groote Eylandt, Port Walcott (run by Hamersley Iron) and virtually all the South Australian ports. There are also 'heritage' ports run by state conservation agencies.

Facilities within ports, such as container terminals and bulk loading facilities, may be run by public or private corporations, and service providers, such as tug companies, are also privately owned and operated. Security requirements are implemented by individual port corporations and facilities. The port authorities have a coordinating role in relation to the other organisations.

State legislation declares the 'port waters' of the port, within which the activities and movement of vessels are under the control of a harbour master. Port limits are shown on large-scale Australian navigational charts. Controls within port waters are published in port regulations, directions and handbooks issued by the port authority or operator.

Decisions on implementing port security arrangements, operations and funding can be complex because of the multiple levels of public–private partnership. Port security is clearly an issue of national security, but because most Australian ports and other critical infrastructure are controlled by state governments, their security is largely coordinated at the state level to meet national requirements. State government involvement tends to vary from state to state.

Risk factors

By their very nature, ports are vulnerable to terrorist attack. They require a sophisticated land transport system and storage logistics capability. They're susceptible because of their size and accessibility, their location in major cities, the amount of material moved through them, and the many transport links to them. These elements must be factored into any security risk analysis.

By their very nature, ports are vulnerable to terrorist attack.

Ports are also essential links in the supply chain. Because of the distances between major ports, the disruption of one port could lead to major disruption and additional economic costs as shippers and importers make alternative arrangements. However, the data to assess the consequences of the disruption or closure of a particular port isn't necessarily available.

Ports differ in their geography, topography, surroundings and population. While individual facilities might not be large, the geographical extent of the port may be very great.

By definition, port facilities are accessible by land and water. They're often located in or near major metropolitan areas and may be intertwined with the infrastructure of urban life, such as roads and bridges. Port facilities in smaller ports may be integral to the social life of the community and extensively used for recreational activity, particularly fishing.

The security regime of a port facility depends on the trade that uses the port. Oil terminals and refinery complexes will already have tight security mainly for safety reasons, but small general cargo or bulk cargo loading ports might traditionally have allowed unmonitored public access to the wharves. Control of access to a port facility is fundamental.

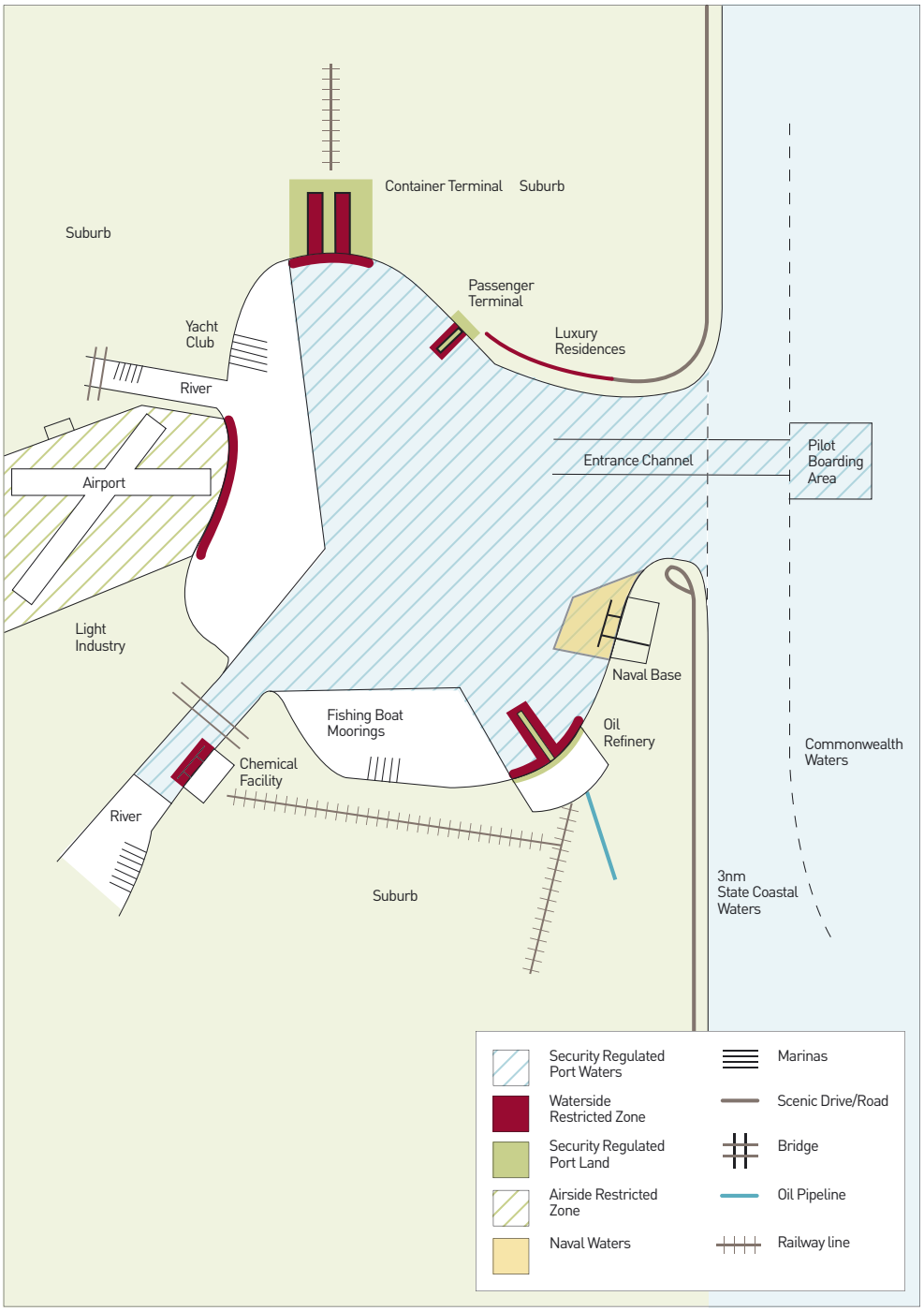
In addition, large merchant ships have very small crews and must depend mainly on the port facility for their security.

The security risk at ports varies widely with their location and size, and with the nature of activities. Similarly, appropriate security responses will vary depending on the assessed level of risk.

Our ports are rich in targets (Figure 2 shows an indicative port system). Attacks could be launched against a ship or port facility from land, from the sea surface or from under water. Attacks on the land side might include multiple coordinated car bombs, improvised explosive devices, or a timed explosive in a shipping container. Attacks on loading and storage facilities for hazardous or volatile materials, particularly those near residential areas, could be attractive options for a terrorist. Oil refineries, terminals and chemical plants are near major population centres in both Melbourne and Sydney, as well as in some smaller ports.

Waterside security will generally be more difficult and costly than landside security. Ports and ships are vulnerable to almost every category of surface or underwater threat, but our major urban ports—with waterways, channels, and commercial and recreational boat traffic—aren't conducive to physical barriers. The threat of mines or the discovery of a mine, particularly in a port such as Brisbane or Melbourne with a narrow entrance channel, could close the port for quite a long time.

Figure 2: Indicative port, showing security regulated port waters and land



Containers and the supply chain

In 2003–04, some 45 million tonnes of general cargo was transported in 4.9 million 'TEUs' ('twenty foot equivalent units'—the standard measure of containerised cargo) (AAPMA 2005). The Australian Customs Service has recently been achieving its target of inspecting 7.0% of more than 3.2 million containers reaching Australian ports from overseas. The sheer volume of container traffic makes inspection of all containers virtually impossible. Refrigerated containers with thick insulation offer particular advantages for concealment. Searching containers only on a random basis would be insufficient, so it's necessary to rely on timely intelligence and on profiling of ports, shippers, cargo receivers, freight forwarders and so on.

Currently, containers are usually sealed with passive indicator seals. The seals don't physically prevent entry but merely indicate whether the container has been opened since it was sealed.

There are many ways that containers can be used for illegal purposes, such as:

- substituting illicit materials for legal cargo
- mixing bogus shipments in a container of multiple shipments
- packing legitimate cargo at the front of a container with illicit material behind
- shipping empty containers with hidden compartments
- shipping a container through one or more transit ports to mask its origin.

Motor vehicles are imported into Australia in specialised car carriers. Car carriers aren't normally seen as being vulnerable to attack, but they may fall in the same category as ordinary shipping containers because terrorist materials might be concealed in a vehicle.

The container transport chain is a massively complex system with numerous players, including shippers, transport operators, specialised terminals and handling facilities, and freight integrators. Terrorists might use different approaches: they could intercept a legitimate consignment and tamper with it (the 'hijack' scenario), or develop a legitimate trading entity to ship a dangerous consignment (the 'Trojan horse' scenario).

Most measures to ensure the security of the supply chain have so far focused on intermediate stages in the chain—the port terminals and the ships. Concern is now shifting to inland carriers and freight integrators operating in the first and last few links of the chain (Willis and Oritz 2004). These might represent a greater security risk than their counterparts nearer the middle of the chain (that is, the terminal operators and ships). These problems are now being addressed by the World Customs Organization, the Asia–Pacific Economic Cooperation (APEC) forum and other regional forums.

Ships

LNG/LPG carriers

The carriage of liquid natural gas (LNG) and liquefied petroleum gas (LPG) by sea in purpose-built ships has increased significantly in recent times. It continues to rise, although growth has been greater for LNG than for LPG, demand for which has tended to level off.

Because gas carriers are modern, 'high-tech' vessels with high value and potentially hazardous cargoes, they're well maintained and operated by highly proficient crews. However, the value of an LNG ship and its cargo, as well as the inherent risks involved and the potential for serious damage through fire and explosion, makes them potential targets. The risks may be higher with LPG carriers, which are smaller and possibly more prone to fire or explosion. It's relatively unlikely that a terrorist group could successfully cause an explosion of an LPG/LNG vessel while underway (Richardson 2004), although a recent investigation by Sandia Laboratories in the US suggests that the risks are still significant because multiple events following an attack on such a vessel could lead to a catastrophic explosion (UPI 2004). However, accidents with gas carriers are generally more likely when loading or unloading than when at sea.

During 2002, Australia concluded its largest-ever single trade deal, to supply $25 billion of LNG to China. The ships carrying this gas will transit through the Indonesian and Philippine archipelagos to a gas terminal in southern China. They will pass through the Sulu Sea between northern Borneo and the southern Philippines, which is a focus of JI maritime activity. Unrestricted access to this direct shipping route is important to the economics of this project, and any need to use a less direct route would add significantly to the costs.

Oil tankers

Australia moves about 15 million tonnes of crude oil and petroleum products as coastal freight each year, while another 28 million tonnes are imported and 22 million tonnes exported. Of concern are cargoes of lighter, more volatile crude oils, as well as refined products such as gasoline, kerosene and diesoline. Oil tankers have little protection from attack, and an oil tanker could itself be used as a weapon. Ships carrying highly volatile cargo, including oil, can't install high-voltage electric fencing to discourage attacks, although one Dutch company has developed a non-lethal system that uses a 9,000-volt pulse to deter boarding attempts.

Chemical tankers

Chemicals are now widely carried by sea, and most oil-producing countries have developed refining and petrochemical plants near main centres of oil production. Seaborne chemicals include inorganic acids and bases, petroleum-derived chemicals (petrochemicals), alcohols and glycols, coal tar products, lubricating oil additives, inorganic chemicals (such as sulphuric, phosphoric and other acids and caustic soda), vegetable and animal oils and fats, and molasses. In the event of an accident, these commodities may pose severe hazards to human life, property and the environment. As demonstrated by the chemical storage and plant facility at Coode Island in Melbourne's docklands, which stores large quantities of explosive and toxic chemicals 1.4 kilometres from the suburb of Footscray and 4.7 kilometres from the city centre, the risks are particularly high when facilities are located near population centres.

Tanker. © APL/Craig Aurness

Bulk carriers

Bulk carriers operate in a very competitive environment, with most time or voyage chartered. Because of the normally low value of their cargo and their relatively low-technology operations, standards of maintenance and crewing may be lower than those for container ships and tankers. High-consequence, hazardous cargoes carried in bulk, including fertilisers such as ammonium nitrate, might be attractive targets or even weapons for terrorists. In 1947, the port of Texas City in the US was devastated when the ship *Grandcamp*, loading a cargo of 2,300 tonnes of ammonium nitrate, caught fire and exploded. In 1917, the *Imo*—with a cargo of dynamite, benzene and picric acid—collided with the *Mont Blanc* in Halifax, Nova Scotia. The subsequent explosion killed 4,000 people and severely injured 8,000 more.

Shipping large quantities of hazardous materials by sea is a relatively safer option than moving them by road or rail. A 'weak link' in the chain is that terrorists could use the low standard of seafarer identification to infiltrate operatives into the crews of foreign vessels. Thorough identity checking needs to be in place to ensure that foreign seafarers are who they claim to be, but the reality is that these checks will never be as reliable as those of Australian seafarers.

High-consequence dangerous goods

Current arrangements for coordinating security for high-consequence dangerous goods in port areas are unsatisfactory. Such goods might be carried as bulk cargo or inside containers. The current Australian Standard for storage and handling of dangerous goods in port areas is based on workplace safety and occupational health, and doesn't cover security. Different standards apply to various elements of the supply chain, including for the sea, road and rail modes of transport. Consistency across the states and modes of transport is important, and there's a strong case that overall responsibility for the ship–port interface should rest with the Commonwealth.

Some dangerous goods entering and leaving Australia are misdeclared to escape the additional costs and administrative measures associated with dangerous cargo. Therefore, it's important to develop a strong regime to license both the importers and exporters, and to ensure adequate packaging and accurate declarations with extreme penalties for violations. The rules for handling dangerous goods vary between the states, but the Australian National Transport Commission is now drafting a new nationwide regime. New regulations for ammonium nitrate, including licensing of the full supply chain, were introduced last year, but they don't address the ship-to-shore interface. It's likely that these will be covered by model legislation to be agreed between the Commonwealth and the states and territories.

Current arrangements for coordinating security for high-consequence dangerous goods in port areas are unsatisfactory.

Because of the vulnerability of the ships carrying high-consequence cargoes, there's a strong case for escorting them while they're moving around in a port and for patrolling around them while they're alongside.

Cruise liners and passenger ferries

Terrorists might see some cruise vessels and ferries as having iconic value. An attack on one of them could cause many casualties and have maximum public impact. These vessels confine hundreds of people in one area and, as was demonstrated by the attack on the *Superferry 14*, the problem isn't so much the direct impact of a bomb but the fire and panic that might follow. In other possible scenarios, a fast ferry could be hijacked and used as a weapon, or passengers on a large cruise liner could be taken hostage.

Actions such as screening passengers and carry-on baggage, inspecting vehicles, improving the security of passenger terminals and having security personnel on board are important, but the ease of access to commuter ferries operating in major cities will still create vulnerabilities. Responsibilities for ensuring appropriate security measures are divided between the Commonwealth and the states, with the national government responsible for cruise liners and interstate ferries, and the states for harbour ferries and local tourist vessels.

Some cruise ships are based in Australian ports; others visit regularly, with Sydney hosting most visits. Passengers and their baggage are now subject to screening and inspection in Australian ports. Vessels calling from foreign ports, including in the Pacific islands, may pose greater risks, although these will be considered when a security risk assessment is undertaken for a particular vessel. Problems might also arise in Australian waters in the Great Barrier Reef, where cruise liners stop at island resorts and other remote locations, and passengers intermingle with people ashore.

The larger harbour ferries, harbour cruise vessels, vehicular ferries or reef cruise vessels in the Great Barrier Reef could be vulnerable to attack. The Circular Quay ferry terminal in Sydney and the Reef fleet terminal in Cairns both handle thousands of passengers each day with little or no passenger screening. Harbour ferries and cruise vessels are also vulnerable

when not in use. Unless the vessels are guarded by security personnel, terrorists could board them and hide a bomb timed to explode when the vessel is full of passengers. To deal with these risks, the Australian Government is now working with the states and the Northern Territory jurisdictions to develop an intergovernmental agreement on surface transport security, including the needs of harbour ferries and cruise vessels.

Crew limitations

Most modern commercial vessels have small crews, with typically about twenty or even fewer personnel crewing a large container ship or oil tanker. This obvious aspect of ship security becomes more critical at higher threat levels. Maintaining an adequate gangway watch is a major problem when the ship's crew is also heavily involved in other activities, including working cargo. The gangway watchkeeper has to deal with visitors, establish their identity and conduct them to their place of business, while also overseeing the gangway, the decks and moorings.

A tanker, loading or discharging at an oil terminal where there are strict security controls ashore, may be less vulnerable than a vessel working general cargo while possibly large numbers of port employees come and go. It might be impractical for a gangway watchman to leave his post to patrol or attend to other ship's business. Similarly, a vessel alongside in a port where there's no possibility of boarding a ship other than by the gangway is less vulnerable than a ship berthed with the main decks level with the wharf, when a swift leap can achieve unauthorised entry.

Warships and naval bases

Naval vessels, like ships generally, are more vulnerable in port than at sea. In port, they face threats from the land, from small boats and from under water. The attack on USS *Cole* demonstrated this vulnerability. The daubing of HMAS *Success*'s side with an antiwar slogan while she was in Wellington in March 2003, and the protesters who attached themselves to HMAS *Sydney* as she sailed for the Gulf in April 2003, also showed the vulnerabilities.

Naval vessels, like ships generally, are more vulnerable in port than at sea.

In September 2004, NSW Police reportedly told the Australian Government that they feared the Garden Island naval base (Fleet Base East) was highly vulnerable to terrorist attack. The police raised a particular concern that, despite new regulations, the Navy hadn't provided small-boat protection against possible water attack. The risks are increased by the proximity of the base to a major road and because it's overlooked by high-density housing.

RAN vessels are bound by rules of engagement that prevent the use of force against protesters. In recent years, there's been an increased naval focus on force-protection training and awareness. The government and the community expect that the Navy should look after its own security. However, for most situations, naval personnel lack the necessary powers, and individual personnel might not have immunity from civil action should they use force.

A naval vessel, including a foreign warship in Australian port, may increase the level of risk in the port and to other vessels berthed nearby. A naval ship visit can compromise

security arrangements and lead to additional costs for other port users if security levels are increased. The RAN and ports have agreed on security measures and communications for RAN vessels in port.

US Navy ships

US Navy ships visiting Australian ports, particularly nuclear-powered vessels, pose additional security problems because terrorists view them as high-value targets. Australian port calls by US warships have long been subject to a policy of 'neither confirming nor denying' the carriage of nuclear weapons. While the US has publicly stated that, with the exception of strategic submarines and supporting ships, 'it is general US policy not to deploy nuclear weapons aboard surface ships, attack submarines and naval aircraft' (USN 1993), this policy statement predates the invasion of Iraq and the War on Terror. The possibility, however slight, that some US Navy ships and attack submarines could have nuclear weapons on board would markedly increase the risks involved.

While OTS requires that the risks associated with foreign warship visits to Australian ports be factored into port security plans, managing the potential risks involved might be beyond the capabilities of the states. Queensland faces a particular challenge in 2005, when major exercises with US forces off the Queensland coast are scheduled and many visits to the state's ports by US Navy vessels, possibly including nuclear-powered vessels, are likely.

Before the visit of a US Navy ship to an Australian port, US embassy and consular officials liaise directly with state and port authorities on security matters. Port calls by US nuclear-powered vessels are managed through the Visiting Ships Panel (Nuclear), and additional security arrangements are always in place (e.g. additional waterborne and land patrols, and standby tug if required); these are probably sufficient.

Offshore facilities

Energy security

Energy security is closely related to maritime security, particularly in a country such as Australia that depends heavily on offshore oil and gas, and whose supplies of energy move largely by sea. Terrorists may recognise this as a significant national vulnerability. Arrangements to protect offshore oil and gas installations, terminal facilities in ports, and oil tankers and gas carriers carrying energy around the coast are major requirements of security against the threat of maritime terrorism. All offshore oil and gas installations are in Commonwealth waters, except for a small area of the Northwest Shelf.

Offshore installations

Australia has about 56 offshore installations, both fixed and floating, in the Timor Sea, Northwest Shelf and Bass Strait. The Northwest Shelf, for example, is one of Australia's most valuable assets, generating billions of dollars of oil and LNG exports. Its importance will grow with the 25-year, $25 billion LNG contract signed in 2002 with China.

Attacks on offshore facilities have occurred. Three offshore Iraqi oil terminals were attacked in the Persian Gulf in April 2003 by explosives-laden speedboats, but these terminals were closer to shore and thus more accessible than Australian installations. The security of onshore pipelines and terminals is another consideration. For example, natural gas from the Northwest Shelf is transported by a 135-kilometre pipeline to the onshore treatment

plant on the Burrup Peninsula, an area that is set to become a major world hub for LNG processing. Projects worth more than $3.8 billion are currently under development on the peninsula.

Australia has about 56 offshore installations, both fixed and floating, in the Timor Sea, Northwest Shelf and Bass Strait.

Currently, the *Maritime Transport Security Act 2003* (MTSA) doesn't cover offshore rigs, although it does cover Australian-flagged offshore mobile drilling units if they can be disconnected from the sea bed and become self-propelled. The government intends to extend the MTSA to cover fixed installations in Australian waters. Only a small proportion of the fifty to sixty floating production ships in Australian waters are Australian flagged.

In the Timor Sea, the current dispute over maritime boundaries with East Timor is making it difficult to implement arrangements for surface protection. This is especially so in waters where Australia has sovereign rights to the sea bed and subsoil resources of the continental shelf but Indonesia has exclusive economic zone rights and obligations. Surveillance patrols in the joint zone, which have been suspended, will presumably resume once there's been agreement on new Timor Sea arrangements with East Timor.

The Australian Government announced in December 2004 that there will be a program of augmented security patrols in the Timor Sea and on the Northwest Shelf. Australia will be seeking the cooperation of Indonesia and East Timor in implementing the patrols.

Offshore structures and floating production, storage and offloading vessels (FPSOs; specially modified tankers that service smaller fields) have few defences against terrorist attack.

Australia's energy security—dependent on maritime security

- Offshore oil and gas production is a major economic use of Australia's marine environment.
- Australia is a major energy exporter—total energy exports in 2002–03 were $24.2 billion, of which $12.3 billion was from oil and gas.
- Australia's energy demand will increase by 50% to 2020.
- Australia's self-sufficiency in crude oil production has fallen from 90% in 2001 to 70% in 2004.
- Over the next decade, self-sufficiency is forecast to drop to somewhere between 20% and 50%.
- Offshore oil and gas supplies 85% of national demand.
- Most major hydrocarbon prospects lie offshore.
- The general trend is from onshore to offshore production and from Bass Strait to the Northwest Shelf and the Timor Sea.

There are vulnerabilities at the points where crew and supply boats dock and helicopters land. Physically getting onto a platform is challenging, but it would be difficult to stop a helicopter determined to land on a rig. The structures could be rammed by a vessel loaded with explosives, but the rigs themselves aren't fragile. To do real damage, the central column would need to be hit, and that isn't easy. Because of the noise at an offshore platform, it would be difficult to detect an underwater swimmer.

Fishing boats and refugee boats have come close to facilities in the Timor Sea. If a refugee vessel were to sink next to a rig and people were to be taken aboard the installation, this would cause the shutdown of production.

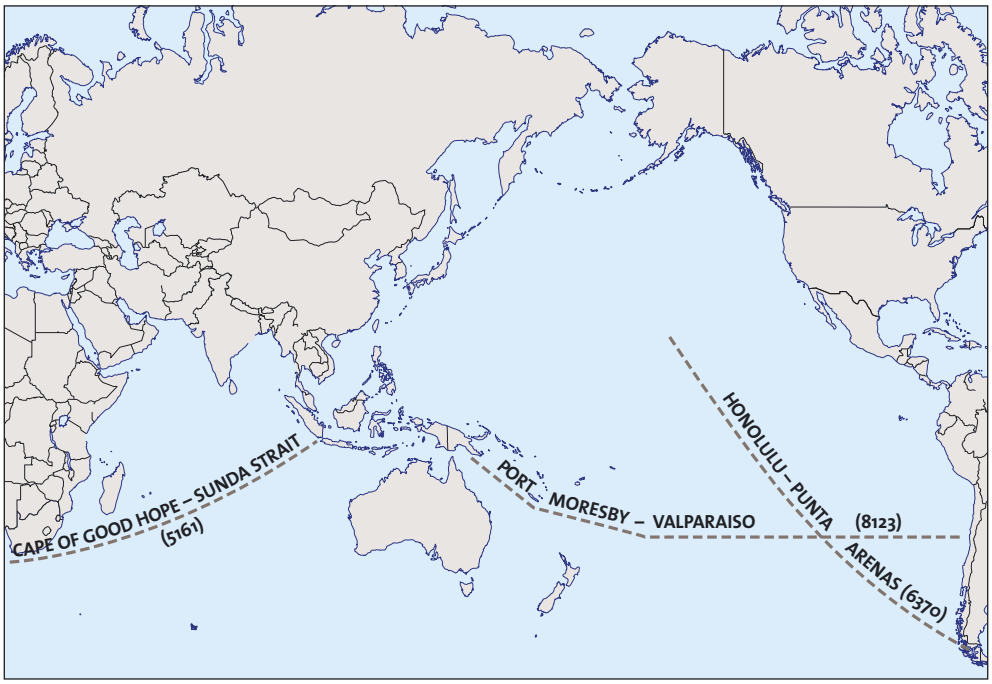
Cables and pipelines

Underwater power cables, while a possible target, would be less attractive than land-based cables. Attacking pipelines is possible, but they're harder to hit than offshore structures. It's also not too difficult to make repairs by looping a pipeline around a break. Again, it would be easier to attack pipelines on land: in recent years, oil and gas pipelines have been attacked in Iraq, India, Russia and Indonesia. In Bass Strait today, there are twenty-two production facilities producing from seventeen fields, connected by a 500-kilometre network of submarine pipelines that carry oil and gas ashore for processing.

Shipping routes

Australia is particularly vulnerable to the disruption of seaborne trade because we are an island continent, our sea lines of communication are long, and ships bound to and from Australia can be easily identified as such at some distance from Australia. For example, iron ore or LNG carriers from northwestern ports passing through straits adjacent to Timor, or bulk carriers with grain or coal from eastern Australian ports using Jomard Passage or Bougainville Strait in the eastern part of Papua New Guinea, are likely only to be travelling

Figure 3: The Sandison Line



to or from Australia. Figure 3 shows the Sandison Line—an imaginary line in the Pacific and Indian oceans, named for an Australian operations analyst. If a ship crosses the line, it can only be heading for a port in Australia, New Zealand or the South Pacific.

Australia's seaborne trade relies on shipping routes through the Indonesian and Philippine archipelagos and the South China Sea. These routes pass through areas where there's a high incidence of piracy and armed attacks against ships and a credible risk of terrorist attack.

Summary of threats

Taking account of vulnerabilities and the relative impact of a successful attack, credible terrorist threats to Australia's maritime security are:

- an attack on an Australian port, either by using a ship as a weapon or by causing an explosion on board a ship carrying hazardous or dangerous cargo
- the sinking of a vessel in a channel or at a berth
- an attack on the loading and storage facilities for hazardous or volatile materials
- an attack on ships transiting the Indonesian or Philippine archipelagos carrying trade to or from Australia
- an attack on an LNG carrier loading cargo at a northwestern Australian port
- a small-boat suicide attack against a high-value target such as a warship, cruise liner, ferry, chemical tanker or oil tanker alongside in an Australian port or moving within the port
- an attack against a cruise liner or passenger ferry, including a harbour ferry
- an attack on a warship, especially a US Navy vessel, alongside in an Australian port, or an RAN vessel in an overseas port
- mining or the threat of mining to close an entrance channel to an Australian port
- smuggling of weapons or equipment, perhaps including WMD, into an Australian port
- infiltration of terrorists and/or their materials into Australia by sea, either by clandestine landing or the use of fraudulent seafarer documentation.

These more credible threats provide a sufficiently diverse basis against which to assess the effectiveness or otherwise of Australia's response to the threat of maritime terrorism. Intentionally, they're more focused than those included in the *Maritime Risk Context Statement* issued by the OTS (DOTARS 2003).

Chapter 3

INTERNATIONAL AND REGIONAL RESPONSES

Introduction

The events of 9/11 have changed the world in many ways. The maritime transportation industry has been greatly affected and now has a vastly different regulatory environment. It's yet to be seen how effective the new measures will be, or indeed how enduring they might be in an international industry that has been characterised by double standards, regulation avoidance and exploitative business practices.

The IMO has done much over the years to regulate international shipping and can point to such successes as fewer shipping casualties and incidences of ship-sourced marine pollution. However, many problems remain, particularly with the failure or inability of some flag States to discharge their responsibilities for vessels flying their flags, in accordance with Article 94 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS).

The IMO has given high priority to the review of international legal and technical measures to prevent and suppress terrorist attacks against ships and to improve security on board and ashore. The aim is to reduce the risk to passengers, crews and port personnel, and to vessels and their cargoes. Areas of concern have been the fundamental one of who owns the ship, and who has effective control to ensure both that the vessel isn't used for terrorist purposes and that it has effective security arrangements in place.

Photo opposite: Detail of ship exterior. © APL/Carl Purcell

Amendments to the SOLAS Convention, including the ISPS Code

Responsibilities of contracting governments

- issuance of International Ship Security Certificates (ISSCs)
- approval of ship security plans
- conduct and approval of port facility security assessments
- approval of port facility security plans
- determination of which port facilities require a port facility security officer
- control and compliance measures

Responsibilities of vessel-owning and/or operating companies

- Ensuring that each vessel obtains an ISSC. This requires the following measures:
  - designation of a company security officer
  - a ship security assessment, including an on-site inspection for each vessel
  - a ship security plan developed for each vessel
  - designation of a ship security officer for each vessel
  - training, drills and exercises, including training for company security officers and ship security officers

Special provisions applicable to ships

- mandatory fitting of each SOLAS ship with an automatic identification system (AIS) that communicates the ship's identity, position, course and speed
- mandatory display of a unique ship identification number (SIN), marked either on the ship's hull or on its superstructure
- issue, by flag state administrations, to each ship of a 'continuous synopsis record' providing information on the ship's name, ship identification number, flag State, date of registration, port of registry and classification society
- mandatory fitting of a ship security alert system to provide a ship-to-shore security alert without raising any alarm on board
- extensive record-keeping requirements, including for records of at least the previous ten port calls

Responsibilities of port facilities

- development and approval of a port facility security plan
- designation of a port facility security officer for each port facility
- Training, drills and exercises for port facility security officers and port facility security personnel

International responses

The international response to the threat of maritime terrorism includes new measures by the IMO, particularly:

- the ISPS Code, which includes both a mandatory section and recommendations
- other amendments to the 1974 SOLAS Convention
- proposed amendments to the 1988 SUA Convention and its Protocol covering offshore facilities
- joint action with the International Labour Organization to develop an up-to-date seafarer identification document and to provide for the security of port areas.

Then there's the range of global initiatives by the US to improve maritime cargo security, especially:

- the Container Security Initiative (CSI), which bases US Customs inspectors in foreign ports to oversee the targeting and pre-screening of high-risk containers bound for US ports (almost two-thirds of all containers that arrive in the US by sea are shipped from 20 top ports, including Hong Kong, Shanghai, Singapore, Kaohsiung, Pusan, Tokyo, Yantian, Nagoya, Kobe, Yokohama and Laem Chabang in the Asia–Pacific region; about 44% of all containers entering the US originate from Asian ports)
- the Customs–Trade Partnership against Terrorism (C–TPAT), which focuses on the security of the supply chain and builds a linked security model within each segment of the chain (production, transportation, importation and distribution), includes customs guidelines for firms and comprehensive security self-assessment, and has evolved to include over 7,400 US companies
- enhanced information management, which requires the presentation of a vessel cargo declaration to US Customs before non-bulk cargo is loaded at a foreign port for shipment to the US (the '24-hour Manifest Rule').

ISPS Code

The ISPS Code came into force on 1 July 2004 (see box for key amendments to the SOLAS Convention, including the code). The code is an agreed international framework that can be extended as appropriate by individual countries. It sets out a systems approach, which takes into account not just the ships but also the ports with which they interact.

Some problems remain with the effectiveness of the ISPS Code as a maritime security measure.

Some problems remain with the effectiveness of the ISPS Code as a maritime security measure.

Some problems remain with the effectiveness of the ISPS Code as a maritime security measure. First, there are still regional pockets in which progress has been slow. Africa, in particular, is falling behind other continents in complying with the new regulations, and countries in the former Soviet Union and Eastern Europe have also made slow progress. Compliance with the code places strong demands on the national shipping administration and the government departments responsible for ports and port facilities. Many developing countries, including Indonesia and the Philippines, are struggling to cope.

Second, the code applies only to so-called 'SOLAS ships' (that is, ships over 500 tonnes gross and passenger vessels employed on international voyages). Unless extended by national legislation, it doesn't apply to warships, government vessels on non-commercial voyages (e.g. scientific research vessels), fishing vessels, ships under 500 tonnes gross, pleasure craft and yachts, or merchant ships employed only in the domestic trade. The number of vessels to which the code doesn't apply is particularly large in Asia, where there are large fishing fleets, many smaller trading vessels and big domestic commercial fleets, particularly in China, Japan, India, Indonesia and the Philippines. In Australia, the Maritime Transport Security Act 2003 extends ISPS provisions to all ships employed on interstate voyages, but not to ones used for intrastate voyages.

Third, the ISPS Code is basically a US code; it is more easily implemented through a single organisation (such as a national coast guard) responsible for national port and ship security. It presents difficulties for other contracting parties. Many developing countries don't accept the priority of measures that are primarily about countering terrorism and securing the interests of major Western countries. They give higher priority to economic development and poverty alleviation, rather than to investing in the capacity to implement the provisions of the code.

Fourth, the ISPS Code is yet another powerful piece of regulation introduced by the IMO that imposes significant additional costs on shipowners, possibly requiring them to employ extra crew (Berkenkopf 2004). The Australian Shipowners Association has estimated that the cost for affected Australian-flagged vessels could be between $750,000 and $900,000 each. This is an extremely high cost penalty, particularly for smaller vessels. Currently, the international shipping market is buoyant, and the costs of the new maritime security measures are being absorbed by the market. Difficulties may emerge with the next slump in global shipping. Some shipowners in developing countries, including national shipping fleets, have already been priced out of the market by the high costs of complying with international shipping regulations.

Last, and despite some rhetoric to the contrary, the ISPS Code, like other instruments of international law, can't be enforced effectively. While Australia might put considerable effort into monitoring compliance, mainly through port state control over foreign-flag vessels seeking entry to Australian ports, other countries might not. The scope for verifying the compliance both of ships and of foreign port facilities may be minimal. The IMO can monitor compliance, but ultimately it all depends on the efficiency of the flag State establishing administrative arrangements for the code and ensuring the compliance of ships flying its flag. The IMO is attempting to establish a system of flag State audits, but these will be voluntary and only as good as the flag State is prepared to make them.

Seafarer identification

There are about 1.3 million international seafarers, and concerns have been raised about terrorists assuming the identities of seafarers to move around the world. The IMO has been working with the International Labour Organization to develop an up-to-date seafarer identification document that must include biometric data. The revised Seafarers' Identity Documents Convention of 2003 provides for a uniform and global identity document to permit the positive, verifiable identification of the seafarer.

However, the convention is problematic. Each state party must permit the entry into its territory of a seafarer holding the identity document, and Australia, for example, might not

ratify the convention because of this concession of visa-free entry. Other concerns relate to the feasibility of the convention's requirements for the physical security of the document and for the basic infrastructure for issue and verification, including maintenance of a national database.

The new seafarer ID documentation also raises important human rights issues. Biometric data can be manipulated, and might be used for other purposes. Seafaring is a demanding occupation, and seafarers should have reasonable access to shore leave without being subject to rigorous security measures that might prevent them going ashore.

SUA Convention

About a dozen international conventions deal with the threat of terrorism, but only the SUA Convention and its protocol relate to terrorism at sea. The purpose of the SUA Convention was to close the gap created by the limited definition of piracy (for example, the international anti-piracy regime doesn't apply to internal waters, the territorial sea and archipelagic waters, or to incidents in which people already aboard the ship as passengers, crew or stowaways are the perpetrators of the crime). The convention extends coastal state enforcement jurisdiction beyond territorial limits, and in particular circumstances allows exercise of jurisdiction in an adjacent state's territorial sea. The relatively low level of ratification of the SUA Convention, particularly in Southeast Asia (only Singapore and Vietnam are parties so far), is probably due to sensitivity about such extraterritorial aspects.

A new protocol to the SUA Convention is under consideration by the IMO, and a diplomatic conference to adopt amendments to the convention and protocol will be held in October 2005. The amendments will include new offences and expanded provisions on ship-boarding: new provisions would allow flag States to request assistance with ship-boarding and law enforcement, or another party to seek the approval of a flag State to board and search a suspect ship claiming the nationality of the flag State. These proposed changes have mainly been at the behest of the US and are designed to overcome potential limits on the conduct of operations at sea as part of the War against Terror.

Security of port areas

A code of practice for the security of port areas, developed jointly by the International Labour Organization and the IMO, recognises the interface between these two organisations on matters of ship and port security. Its aim is to maintain an acceptable level of risk at all security levels. Some examples of security measures that may be considered are those that will:

- prevent access to the port by people without a legitimate reason to be there
- prevent people with legitimate reasons to be in the port from gaining illegal access to ships or other restricted port areas for the purpose of committing unlawful acts
- prevent the introduction of unauthorised weapons, or dangerous or hazardous substances and devices, into the port or vessels using the port
- prevent personal injury or death, or damage to the port, port facility, ship or port infrastructure by explosive or other devices
- prevent tampering with cargo, essential equipment, containers, utilities, protection systems, procedures and communications systems affecting the port
- prevent smuggling of contraband, drugs, narcotics, other illegal substances or prohibited material

- prevent other criminal activities, such as theft
- protect against the unauthorised disclosure of classified material, proprietary information, or security-sensitive information.

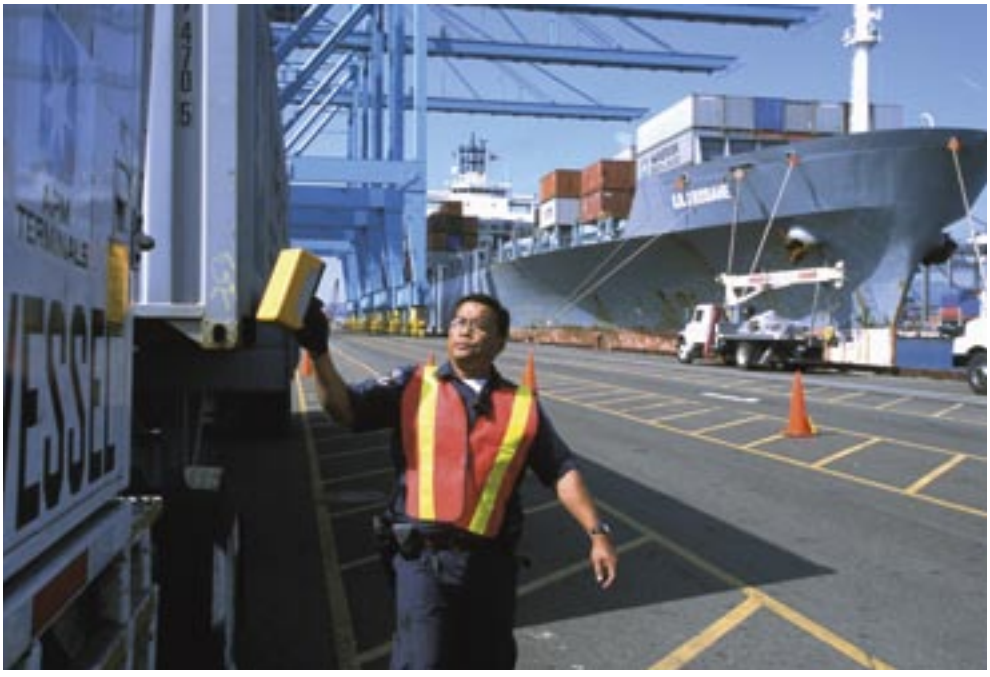
The new code of practice isn't a legally binding instrument and isn't intended to replace national laws and regulations. It isn't intended to affect the fundamental principles and rights of workers provided by International Labour Organization instruments, or the facilitation of workers organisations' access to ports, terminals and vessels.

Since 9/11, the US has attached considerable importance to securing its national transportation system from terrorist attack.

US maritime security initiatives

Container Security Initiative

Since 9/11, the US has attached considerable importance to securing its national transportation system from terrorist attack. A major concern has been to prevent the system being used to introduce terrorists or their materials into the US (a WMD, in the worst case). The major initiatives for ships and their cargoes have been the CSI and C–TPAT. Core elements of the CSI include the establishment of new security criteria to identify high-risk containers and the introduction of new technology to screen containers and make containers more secure. Other requirements of the US include the requirement for a foreign vessel to have a valid ISSC to enter a US port, and for a ship's previous port of call to have in place valid anti-terrorism measures that are open to audit by US inspectors.



A US Customs and Border Protection officer scans containers at the LA and Long Beach complex. © APL/Ed Kashi

These US maritime cargo initiatives have encountered some resistance. Countries that don't implement required CSI procedures will be disadvantaged because their shipments will be subject to more complex examinations and will be cleared more slowly. Therefore, the playing field isn't level, and countries that can afford the new measures will gain significant comparative advantage. To put it bluntly, unless adequate programs of technical cooperation and financial assistance are available, 'the rich will get richer and the poor poorer'. US rhetoric that CSI and C–TPAT 'push out the borders' also sends the wrong message, implying that these measures only serve to export the terrorist threat away from North America.

Proliferation Security Initiative

The Proliferation Security Initiative (PSI) seeks to establish a coalition of willing partners to respond to challenges posed by the proliferation of WMD. It involves a set of principles, available on the websites of the US Department of State and the Australian Department of Foreign Affairs and Trade, identifying practical steps to interdict shipments of WMD flowing to and from state or non-state actors 'of proliferation concern'. The fifteen full members (the 'core group') of PSI are Australia, Canada, France, Germany, Italy, Japan, the Netherlands, Norway, Poland, Portugal, Singapore, Spain, Russia, the UK and the US), but more than sixty countries have indicated support for the initiative. Only two Asian countries (Japan and Singapore) are full members. Others have expressed scepticism about the value and appropriateness of the PSI.

The PSI promotes new international agreements that allow the US and its partners to board and search ships suspected of carrying WMD or associated materials. Ship-boarding agreements have been signed between the US and Liberia, Panama and the Marshall Islands that permit the boarding of ships flying the flags of those countries. Similar agreements are sought with other major flag States. These are premised on the principle that boarding requires the consent of the flag State of the suspect vessel. Presumably Australia, as a member of the core group, will seek similar ship-boarding agreements with flag States.

Regional Maritime Security Initiative

The US has promoted the Regional Maritime Security Initiative (RMSI) to improve international cooperation, specifically in the Malacca Strait, against the transnational threats of terrorism, piracy and trafficking. Major elements of RMSI include increased situational awareness ('maritime domain awareness'), information sharing, a decision-making architecture, and interagency cooperation.

Malaysia and Indonesia were both initially opposed to the implementation of RMSI, but this opposition may have been based on a misunderstanding of what the US was proposing. Discussions are proceeding. The US has emphasised that the RMSI doesn't interfere with national sovereignty and aims to rely on existing laws and forces. There's no presumption that US forces will have an operational role. The June 2004 agreement between Indonesia, Malaysia and Singapore to establish coordinated patrols in the Strait of Malacca might be seen as a response to the RMSI, and a demonstration that littoral countries are committed to maritime security in the strait.

Current regional capacity

At present, the region lacks effective arrangements and the necessary capacity to provide for the safety and security of shipping, and to generally maintain law and order at sea. Current weaknesses include lack of political and social will, lack of maritime awareness, ineffective

arrangements for maritime jurisdiction and enforcement, differing interpretations of the Law of the Sea, weak regional participation in relevant international legal instruments, and lack of capacity to implement appropriate measures.

At present, the region lacks effective arrangements and the necessary capacity to provide for the safety and security of shipping, and to generally maintain law and order at sea.

At a national level, many regional countries lack the capacity to provide adequate security in waters under their national jurisdiction and to implement international standards for ship and port security. New international measures are generally optimised for developed countries and challenge the capacity of developing countries that might have other national priorities.

At a regional level, the region lacks established procedures and frameworks for information exchange, and for operational coordination to provide both maritime security and maritime safety. Bilateral sensitivities continue to inhibit cooperation between the maritime security forces of neighbouring countries, and there's a lack of established arrangements for cooperation—both between neighbouring countries and between the coastal states and the 'user' states whose ships and trade pass through the waters of the coastal states.

Regional responses

Both the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) and the APEC forum have initiated action to improve the safety and security of shipping and seaborne trade. The *Statement on Cooperation Against Piracy and Other Threats to Maritime Security*, produced by the Tenth ARF held in Phnom Penh in June 2003, provides a clear statement on how forum participants should work together to protect ships engaged in international voyages. The text of the statement is available on the website of the Department of Foreign Affairs and Trade.

APEC has been active in developing regional responses to the threat of maritime terrorism. In February 2003, the organisation endorsed a Counter-Terrorism Action Plan listing specific objectives and expected outputs by APEC economies to secure cargoes, protect people in transit, secure ships engaged in international voyages, ensure the security of international aviation, halt the financing of terrorism, enhance cybersecurity, secure energy supplies and protect the health of APEC communities. The plan encourages all APEC members both to identify their capacity-building needs and to outline the expertise they can offer other members.

The Secure Trade in the Asia–Pacific Region (STAR) initiative developed by APEC provides for the protection of ships and cargoes, promotes the introduction of ship and port security plans, provides for the accreditation of seafarer manning agencies in the region, promotes cooperation on fighting piracy, sets standards for shipborne detection equipment and technology, and pays particular attention to energy security, including the security of sea lines of communication.

The APEC High Level Meeting in Maritime Security Cooperation, held in Manila in September 2003, drew up an indicative list of capacity-building needs of APEC economies for the implementation of maritime security measures, and agreed to present this list to international financial institutions. At the APEC summit held in Santiago, Chile, in November 2004, President Bush and six other leaders, including Prime Minister Howard, launched the ISPS Code Implementation Assistance Program to help APEC members comply with the ISPS Code through technical assistance and grants.

Japan Coast Guard

The Japan Coast Guard is one organisation that in recent years has been extremely active in regional maritime capacity-building. The coast guard offers training for foreign personnel in Japan, helps Southeast Asian countries develop their own coast guards, and has hosted port security seminars in Southeast Asia to assist implementation of the ISPS Code.

The Japan Coast Guard took a leading role in the development of the Asian Maritime Security Initiative 2004, agreed at a June 2004 meeting of the heads of Asian coast guards in Tokyo, and the more recently agreed Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP). All ASEAN nations, Japan, China, Korea, India, Bangladesh and Sri Lanka are working under ReCAAP to set up an information network and a cooperation regime to prevent piracy and armed robbery against ships.

Japanese Coast Guard vessel. © Defence Department

Chapter 4

THE AUSTRALIAN RESPONSE

Introduction

In July 2004, the Australian Government announced a series of new maritime security measures worth $102 million over four years (see box on page 49). These added to major initiatives already taken by the government, including the prompt and effective implementation of the ISPS Code in Australia, additional border protection and tighter immigration arrangements at seaports. Until mid-2003, the major focus of counter-terrorism initiatives in the transport sector had been aviation security, but the IMO's development of the ISPS Code triggered attention to maritime security.

Most recently, in December 2004, the government announced plans to establish a new Joint Offshore Protection Command and a Maritime Information System extending up to 1,000 nautical miles from Australia's coastline. Australia's maritime security environment is now vastly different from what it was just two years ago.

Australia has significant resources at the national, state and local levels to protect the community from global terrorism, including maritime terrorism.

Australia has significant resources at the national, state and local levels to protect the community from global terrorism, including maritime terrorism. The challenge is how best to marshal those resources to ensure that gaps are identified and corrected. This requires a good

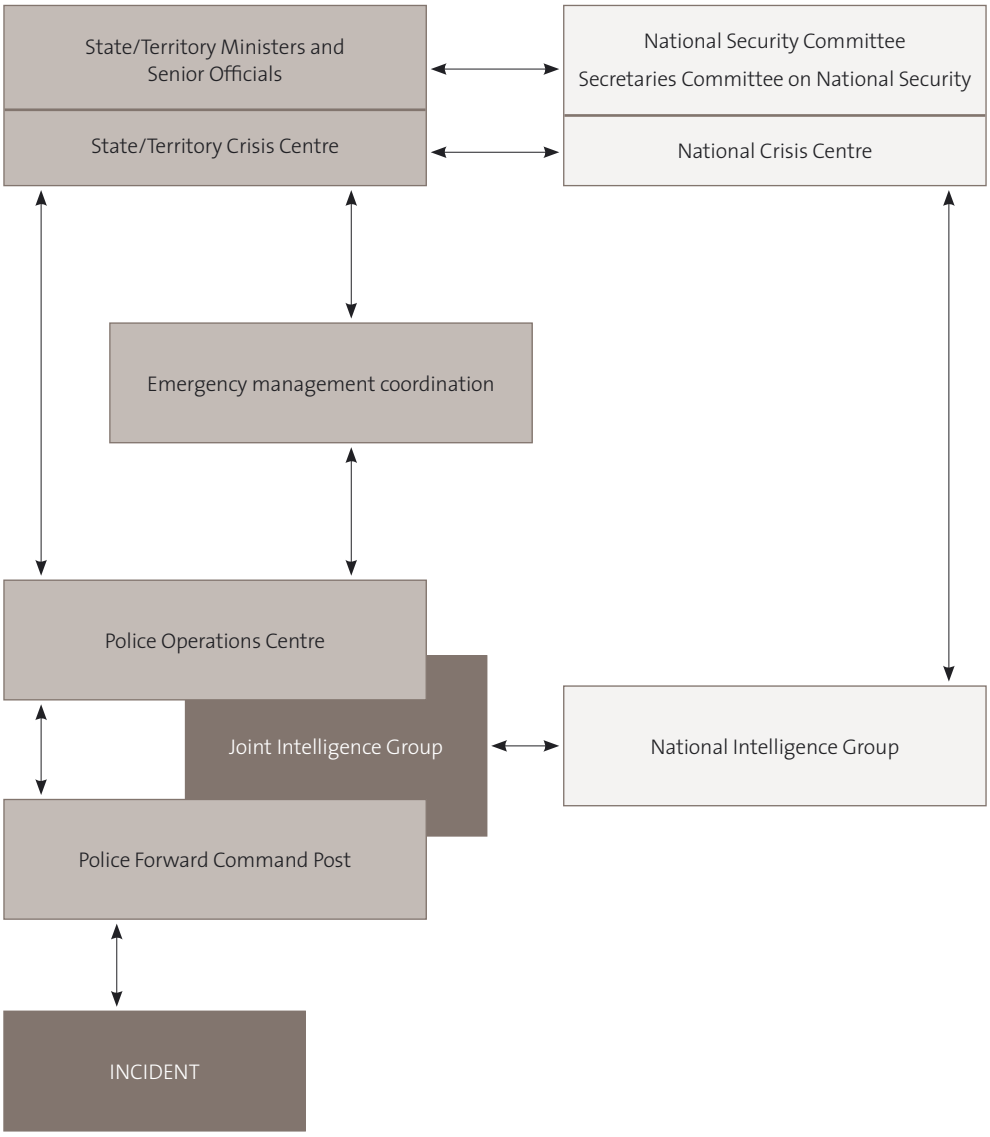
Photo opposite: HMAS *Adelaide* departs Fleet Base West for Operation Catalyst in the Persian Gulf, July 2004. © Defence Department

understanding of the bureaucratic, organisational and legal barriers that must be overcome so that diverse private and public sector bodies can coordinate their efforts. It also requires information sharing, without compromising security or swamping agencies with data, so that terrorist actions might be prevented or the damage can be contained if they occur.

National counter-terrorism policy

The National Counter-Terrorism Plan (NCTP) was released in June 2003. The plan outlines responsibilities, authorities and the mechanisms to prevent acts of terrorism (including maritime terrorism) in Australia or manage their consequences. The Protective Security Coordination Centre (PSCC) in Canberra has responsibility for operational coordination of national counter-terrorism arrangements. The *National Counter-Terrorism Handbook*, which sets out in detail relevant procedures and protocols, supports the NTCP. In mid-2004, the

Figure 4: Counter-terrorism management arrangements



Note: States and Territories have different arrangements to coordinate consequence management.

government released the *Transnational Terrorism: the Threat to Australia* White Paper and established a Taskforce on Offshore Maritime Security, whose report led to the new Joint Offshore Protection Command.

In any terrorist attack on a port, ship or other maritime target, operational arrangements under the NCTP would be activated. Civil police would assume control, and the matter would remain a civil one unless the resolution of the threat was beyond the capacity of the civil authorities—in which case a state or territory could apply for Defence assistance (see below). If the situation were serious enough, the Australian Government would assume overall responsibility for policy and broad strategy, in close consultation with relevant states or territories.

New maritime security measures

The government's additional maritime security measures announced in July 2004 included:

- providing additional resources enabling the Customs National Marine Unit to double the time its vessels are at sea each year
- introducing a Maritime Security Identification Card for maritime industry employees
- increasing the rate of container examination, with a fifth X-ray facility to be built in Port Adelaide and additional machines in Melbourne, Sydney, Brisbane and Fremantle
- providing an extra $75 million in funding to take the number of containers screened each year from 80,000 (5%) to 100,000 (7%)
- enabling Customs to board more vessels at their first port of arrival and to include more random checks
- posting specialist immigration officers to ports to help detect passport fraud
- extending the Customs closed circuit television network from the current thirty-two ports to sixty-three customs-proclaimed ports
- amending the Migration Act to allow for more checks on cruise ship passengers
- providing additional limited powers for privately engaged maritime security guards
- providing additional resources to further strengthen intelligence collection and the provision of intelligence information in key ports
- providing funding for the Transport Security Operations Centre to operate twenty-four hours a day for the next four years.

During the 2004 federal election campaign, the Australian Government committed to buying two additional Armidale Class patrol boats for dedicated surveillance and monitoring of the Northwest Shelf. The government is also to invite two defence companies to participate in a trial to assess the maritime surveillance potential of Global Hawk and Mariner unmanned aerial vehicles, including their ability to operate with patrol boats to protect the Northwest Shelf environment.

The National Counter-Terrorism Committee (NCTC) is the key body for interjurisdictional policy coordination and nationwide capability development. The committee comprises senior representatives of relevant Australian Government agencies (DOTARS is a member), state and territory premiers' and chief ministers' departments, and police services from each jurisdiction. It coordinates nationwide counter-terrorism capability, provides strategic and policy advice to government, and maintains arrangements for sharing relevant information between jurisdictions. There's also a transport security policy committee reporting to the NCTC.

Who are the stakeholders?

Federal stakeholders

DOTARS provides policy advice on commercial shipping matters and administers relevant legislation. It includes the OTS, established in December 2003 as the principal security regulator for the maritime sector, and a 24-hour Transport Security Operations Centre. The OTS has significantly increased its staff over the past year, from around seventy to about 220, including people outposted in the states and overseas.

The Department of Defence hasn't previously had direct maritime security responsibilities (other than for naval bases, naval or military ships, and naval waters), but under the new offshore security arrangements announced in December 2004 the ADF will take direct responsibility for offshore counter-terrorism. This includes the protection of offshore oil and gas facilities and the interdiction of suspicious vessels.

The Australian Customs Service is responsible for preventing the importation of illegal goods and for border protection generally. It also controls the National Marine Unit of Customs vessels.

Coastwatch is a division of Customs, with an RAN two-star officer seconded as its Director-General. Coastwatch coordinates the civil maritime surveillance program and surface response operations, using either RAN or Australian Customs vessels. The Director-General Coastwatch will become 'double-hatted' as the Commander of the Joint Offshore Protection Command, responsible to the Chief of Defence Force for the command's military functions and to the chief executive officer of Customs for its civil functions.

The Attorney-General's Department includes ASIO, which provides intelligence and threat assessments for ships and ports. The department also has a coordination role through the PSCC. The Critical Infrastructure Protection Branch is responsible for the development and coordination of Australian Government policy and international cooperation related to critical infrastructure protection.

The AFP is responsible for Commonwealth law enforcement, often in conjunction with state police forces. The AFP plays a lead role in counter-terrorism arrangements, including preventing follow-up attacks and investigating any attack. The AFP Protective Service provides protective security services for the Australian Government. The Australian Bomb Data Centre provides technical intelligence and advice on devices and components.

The Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) manages immigration programs and the entry of individuals into Australia.

The Australian Maritime Safety Authority is the operational Commonwealth authority for maritime safety, including port state control and search and rescue.

The Australian Quarantine and Inspection Service (AQIS) is involved in border protection to prevent the spread of exotic diseases through the importation of infected insect, animal or vegetable material.

Emergency Management Australia, part of the Attorney-General's Department, has a national coordinating responsibility for emergency preparedness and response in the event of a terrorist attack.

The Department of Health and Ageing would be involved in some biological and chemical scenarios, as would AQIS and the Australian Radiation Protection and Nuclear Safety Authority.

The Department of Environment and Heritage may be involved in determining the type and scope of environmental damage, and has policy responsibility for such marine installations as floating hotels, tourist pontoons and artificial islands.

The newly formed National Offshore Petroleum Safety Authority administers offshore petroleum safety legislation and so would be involved in preventive measures relating to security threats to offshore structures.

The Department of Industry, Tourism and Resources is responsible for offshore oil and gas installations, although when FPSOs are detached from their moorings they come under Australian Maritime Safety Authority.

The Department of Communications, Information Technology and the Arts will administer a new submarine cables protection regime.

State and local government stakeholders

The state marine safety or administrative agency (the actual title of the agency varies from state to state) has responsibility for the safe operation of vessels, navigational safety, community awareness, vessel registration and operational requirements, and marine oil-spill responses.

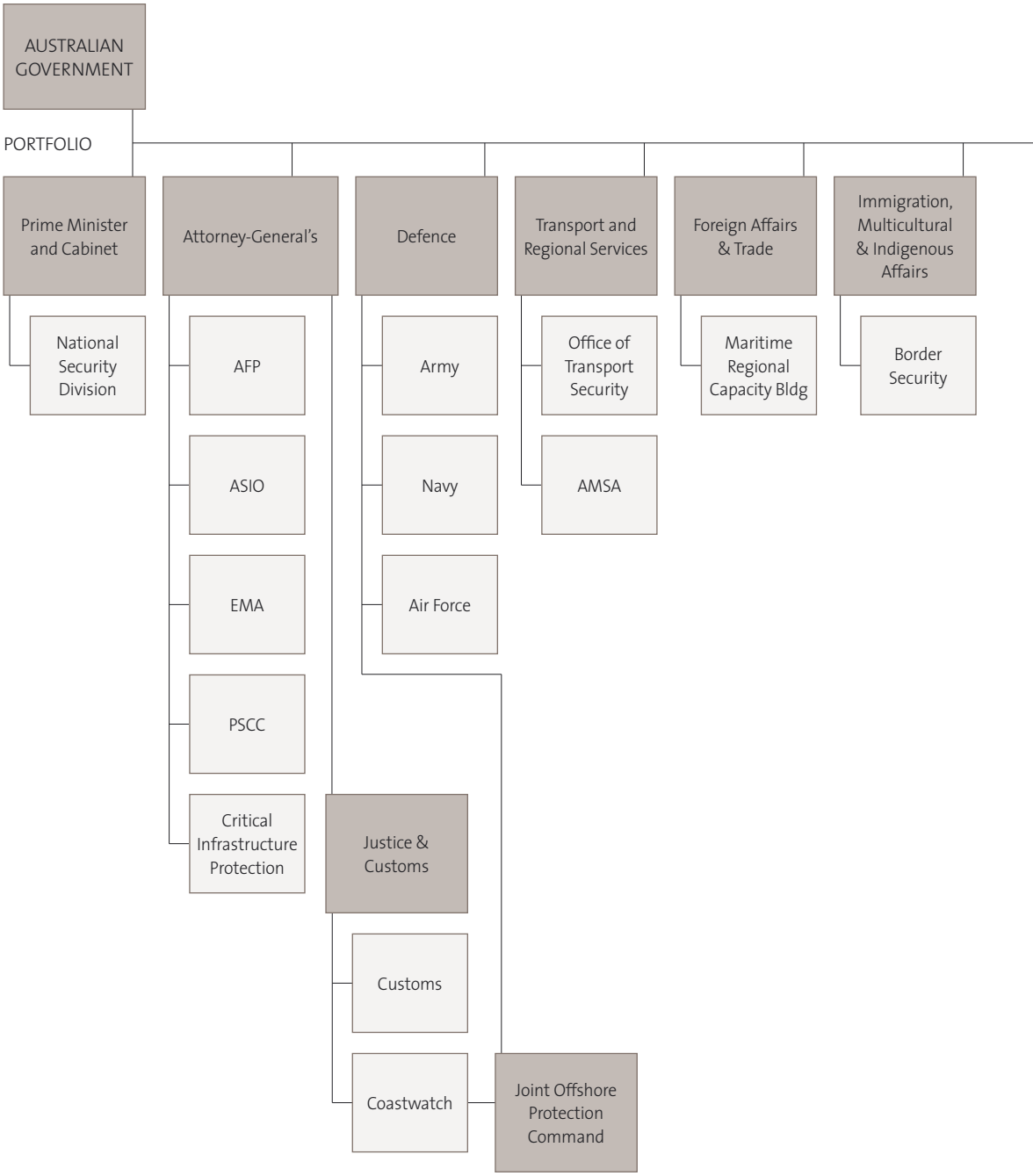
Port authorities or corporations are responsible for the successful operation, regulation and security of port facilities, and coordinate actions for port facilities owned by others. They mainly rely on private security firms as their enforcement bodies. They usually have emergency service units, trained for hazardous material response, water rescue and fire, that may be important in the event of a terrorist attack.

State police services are critical in providing first-response capabilities at or near ports in their jurisdictions.

State police services are critical in providing first-response capabilities at or near ports in their jurisdictions. The police, including water police, and fire brigades would be the first responders at the scene of any attack. Police assume control when there's reasonable suspicion that an incident is terrorism related.

In most states, the Premier's Department provides the coordinating machinery to oversee and implement the state's counter-terrorism strategy.

Figure 5: Federal stakeholders



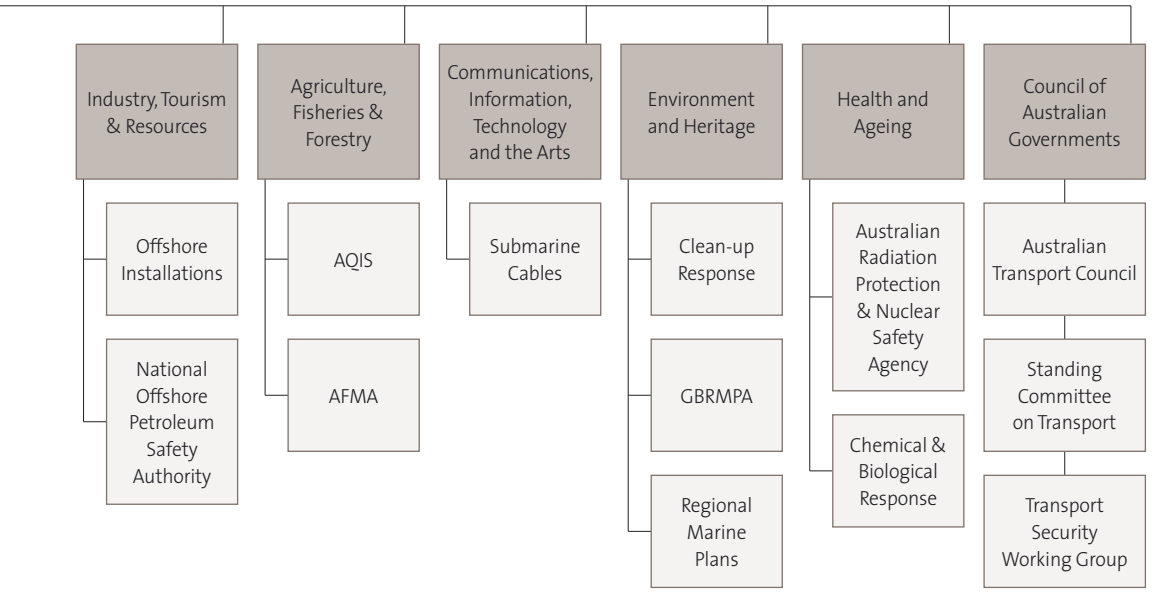
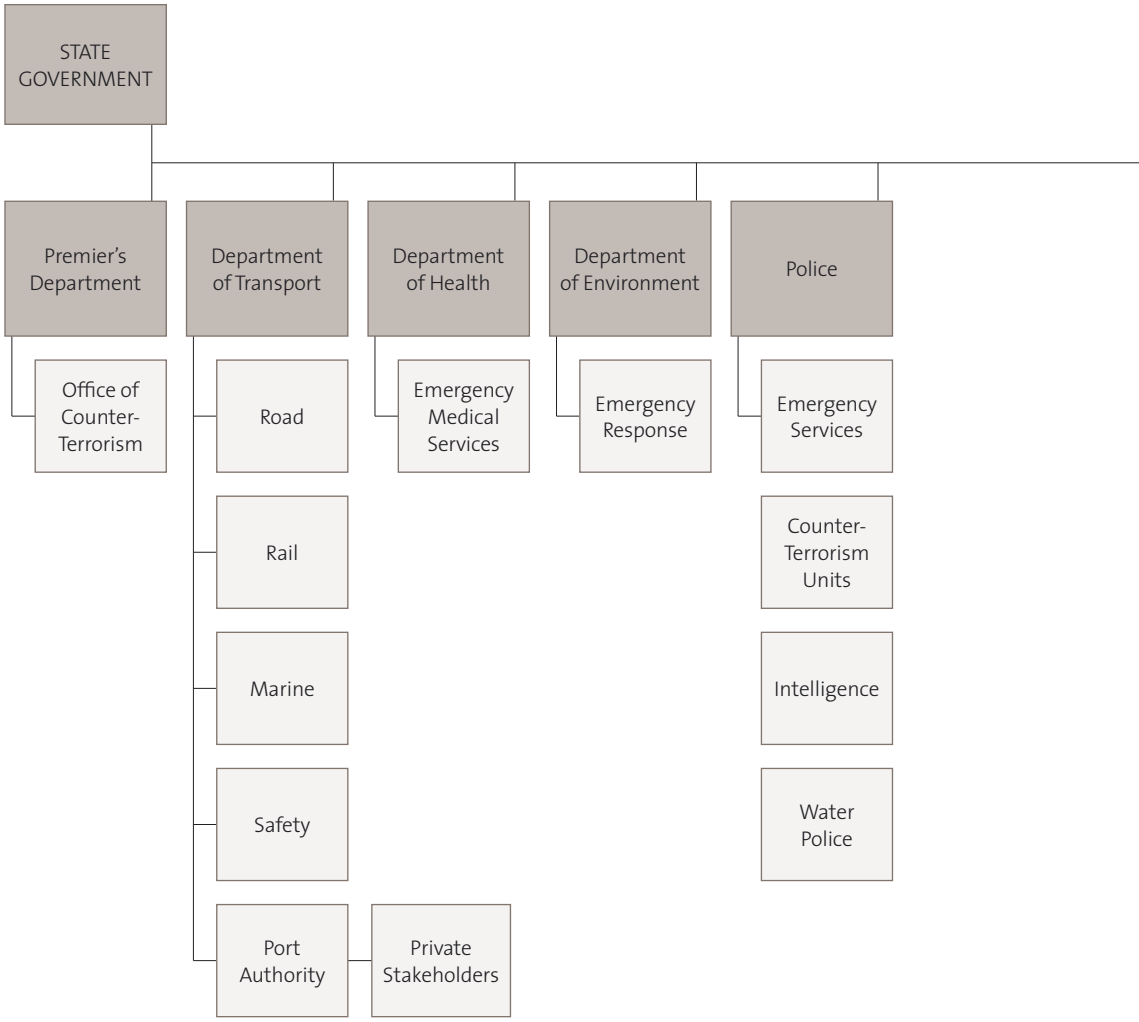

Industry, Tourism & Resources
Offshore Installations
National Offshore Petroleum Safety Authority
Agriculture, Fisheries & Forestry
AQIS
AFMA
Communications, Information, Technology and the Arts
Submarine Cables
Environment and Heritage
Clean-up Response
GBRMPA
Regional Marine Plans
Health and Ageing
Australian Radiation Protection & Nuclear Safety Agency
Chemical & Biological Response
Council of Australian Governments
Australian Transport Council
Standing Committee on Transport
Transport Security Working Group

Figure 6: State stakeholders



The states' emergency management services are responsible for coordinating remediation efforts in the event of an attack, and are normally encouraged by state police to contact the police in the event of suspicious activity around ports or other vital installations.

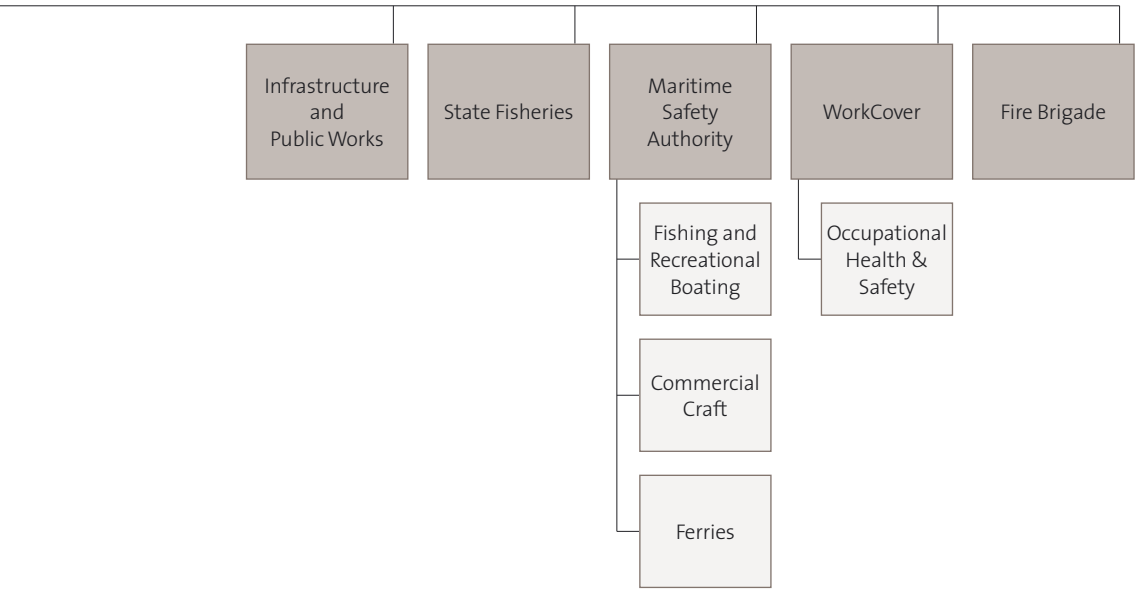
State departments of health may play a role in the detection of some types of terror attacks on ports, and also during the response by coordinating emergency medical assets.

Some states have departments of infrastructure and public works that would be involved in prevention and remediation efforts.

State WorkCover agencies are involved in port safety issues that have security implications, such as the handling of dangerous substances.

State environmental agencies would be involved if an attack were to have environmental implications.

Because every port is different, the stakeholders involved might vary according to the port. A number of ports have waterways that run into them, so that state waterways authorities would be involved in port access control. For example, the NSW Maritime Authority is



responsible for ports at Eden and Yamba, the Victorian Channel Authority is responsible for provision and management of channels and port waters at Victorian regional ports, and the Port of Melbourne Corporation is responsible for the entry channels into Port Phillip.

Because railways and roads run into several ports, state rail and road authorities also have a vital role in consequence management and in port security planning arrangements. In some jurisdictions, bridges could be destroyed that would block ports, involving state public works authorities.

Because most ports are in major cities, often next to major residential areas, the local government role in health, road maintenance, traffic control and sanitation would also be important in certain situations. Local government would be critical in maintaining public confidence in the event of a major incident at one of our larger ports. Local governments may also grant building permits adjacent to port precincts that have security implications. In a number of states, local government legislation empowers councils, with the approval of the port operator or relevant minister, to make by-laws in relation to part or all of a port or to adjacent land.

Private stakeholders

Private stakeholders include shipping and stevedoring companies, terminal operators, shipping agents, protection and indemnity clubs, insurance companies, classification societies and tug companies. Key non-government associations are:

- the Australian Shipowners Association, representing Australian companies that own, operate and/or manage seagoing ships
- Shipping Australia Limited, the industry body representing the interests of major Australian and international shipowners and operators, and companies involved in the full spectrum of shipping trades
- the Association of Australian Port and Marine Authorities, the peak body representing the interests of member ports and marine authorities
- the Australian Peak Shippers Association, representing exporter interests
- the Australian Petroleum Production and Exploration Association, representing the interests of companies involved in oil and gas exploration and production operations in Australia and companies that provide goods and services to the upstream petroleum industry
- the Australian Logistics Council provides leadership within the freight logistics industry by encouraging industry collaboration on issues of mutual interest
- the Maritime Union of Australia, with 10,000 members (98% of waterside workers are members of the union).

There are indirect stakeholders in port security, such as the shippers who use a port. More directly involved are the shipping firms and stevedoring and container companies that have facilities at the port, shipping agents, and those who own the refineries, terminals and other critical infrastructure. Other stakeholders would be companies supplying ancillary port services, such as mooring and unmooring of vessels, security services, quarantine and non-quarantine waste collection, and sea pilot services.

The legal setting

New maritime security law

The *Maritime Transport Security Act 2003* (MTSA) gives effect to Australia's implementation and interpretation of the ISPS Code. Under this new legislation, the Australian Government regulates the security arrangements of Australian ports, port facilities (defined as areas within security-regulated ports), and Australian-owned or flagged ships. The legislation extends ISPS provisions to all ships employed on interstate voyages, but not to those used for intrastate voyages. The legislation also establishes robust compliance checking of foreign ships, which must provide pre-arrival information forty-eight hours before entering an Australian port.

The MTSA requires the development of individual security assessments and security plans by port authorities, port facilities and Australian-flagged or owned ships engaged in international or interstate trade. All 248 port and port facility plans, which are based on standard risk management practice such as in Australian Standard 4360, were approved by DOTARS by 1 July 2004. In some ways—by establishing security zones in restricted areas, incorporating the criminal code in the legislation, creating a demerit points system, using injunctions and applying high penalty levels—the MTSA goes beyond the preventive

measures in the ISPS Code. Some four hundred maritime industry participants, including port operators, port facility operators, some port service providers and ship operators, are now covered by security plans.

The MTSA includes the most comprehensive security standards ever applied to the operations of Australian ports and ships. The Act demands that DOTARS exercise regulatory authority in the maritime sector far beyond any the department has ever exercised in the past. All ships entering Australian ports are required to have an International Ship Security Certificate (ISSC), and compliance is high. Visiting ships without ISSCs are issued with control directions under the MTSA. To date, six control directions to foreign ships (flagged by Denmark, Vanuatu, Liberia, Cyprus and Panama) and two security directions to Australian ships have been issued. Australia has taken a firm stance on ISSCs: re-entry won't be permitted without a certificate.

Ships subject to the MTSA are required to fit an automatic identification system (AIS) that allows them to be identified by other ships or security authorities ashore. Other vessels aren't required to fit these systems (the small outboard runabouts that attacked the USS *Cole* and the MV *Limburg* were well outside any requirement to have an AIS). The Maritime and Port Authority of Singapore is currently developing a harbour craft transponder system, which will be the small-vessel counterpart of the AIS. However, the transponder system is needed because of the high level of small-craft traffic in and around the port of Singapore, and at this stage isn't justified by the level of activity in any Australian port.

Port restricted waters

Port security plans are drawn up under the MTSA and approved by the OTS. They relate to activities within a declared security-regulated port area, covering the port, ships, land and the waterside. Exclusion zones can be declared around vessels as they move within the restricted port area and around some berths. Waterside restricted zones are indicated by large security warning signs facing the water, on port maps and in other publications or notices. Access may be controlled by maritime security guards and water patrols where such assets are available. Landside restricted zones are normally marked by security fences and warning signs, and access through security gates is controlled by guards. Significant criminal penalties now apply to people who violate port security.

Harbour masters

Within port waters, the harbour master acts as a safety regulator to ensure the safe and efficient movement of shipping. Harbour masters are generally empowered under state legislation with extensive powers to control vessels in port areas. Their powers can in some cases extend to security. They include the power to direct and control the time and manner in which a vessel may enter or leave port waters, the navigation of vessels within the port, the place any vessel may anchor or moor, and the removal of vessels from ports. Harbour masters in some ports can invoke exclusion zones under their own by-laws, rather than under MTSA legislation. They also have some powers covering the land side of the port through port regulations and by-laws.

Foreign seafarers

The type of visa issued to a foreign seafarer depends on the nature of the voyage of the vessel and the activities of its crew. Where a commercial vessel enters Australia as part of an international voyage or under a coastal trading permit, crew are granted a special purpose

visa, provided they hold both a valid passport and a seafarer's identity document at the time of the vessel's arrival in Australia. The crew of foreign vessels engaging in the coastal trade under a single voyage permit or a continuing voyage permit hold special purpose visas for three months. DIMIA regards business long-stay visas as the most appropriate visas for crew members of some special types of vessel, such as cable layers and fisheries research vessels, which may operate in Australian waters for longer periods and periodically enter Australian ports.

Port state control

The Australian Maritime Safety Authority conducts port state control inspections to ensure that ships visiting Australian ports are seaworthy, don't pose a pollution risk and comply with relevant international safety regulations. The authority's officers are authorised officers under the MTSA. Australia is party to the memorandums of understanding on port state control in the Asia–Pacific and Indian Ocean regions. Inspections for security control are separate. They're carried out in relation to maritime security requirements by DOTARS or by other agencies such as Customs, acting on behalf of DOTARS and guided by the MTSA.

Maritime security guards—move-on powers

The MTSA acknowledges that police are the most appropriate authority to exercise powers over people, vehicles and vessels in a maritime security zone without authorisation. The government has now decided that private security guards, known as maritime security guards, should also be able to exercise limited 'move-on' powers. It's envisaged that the MTSA will be amended to give guards the power to ask a person to leave a maritime security zone if they're not authorised to be there. It isn't clear if more coercive powers for guards to detain vessels and vehicles, or to move them out of a maritime security zone, would be legally supported.

Oil rigs and offshore structures

Safety zones extend for a radius of 500 metres around fixed installations. Entry is prohibited to all except authorised vessels. Production platforms and exploration rigs maintain a continuous watch on VHF and will attempt to make contact with any ship entering a declared 'area to be avoided' or heading towards an installation. In Bass Strait, there's a traffic separation scheme designed for the protection of installations. It consists of a 1.5 nautical mile separation zone in the eastbound and westbound shipping lane. Ships of more than 200 tonnes gross are required to avoid the area.

Submarine cables and pipelines

The Australian Government is currently proposing to legislate for specific protection zones over submarine telecommunications cables of national importance. Up to 98% of international voice and data traffic to and from Australia is carried by sub-sea cables, thirteen of which land in Australia. Protected zones will generally be two nautical miles wide and extend from the shore to the edge of our exclusive economic zone. Within the protection zones, activities that are dangerous to cables, such as anchoring, dredging and dumping, will be prohibited; other activities, such as petroleum exploration and the installation of gas and oil pipelines and electricity cables, will be restricted. Criminal penalties will apply within the protected zone for breaking or damaging a submarine cable, and for engaging in prohibited or restricted activities.

Role of Defence

Under the Defence Assistance to the Civil Community (DACC) provisions of the Defence Act, the ADF may be called upon to provide emergency and non-emergency assistance to the government and the Australian community in non-combat related roles. Tasks may include search and rescue, disaster recovery, surveillance and security, and non-emergency law enforcement. Local ADF commanders are authorised to provide emergency support under DACC after receiving a request from civil authorities.

DACC doesn't authorise the use of force. If force may be required, such as in a terrorist attack in state waters, the ADF may be called out under Part III AAA of the *Defence Act 1903* (Defence Force Aid to the Civil Authority, or DFACA). This provision was amended in 2000 to cover the use of the ADF against 'domestic violence', which can be interpreted as widespread criminal activity, including terrorism, likely to threaten national or state interests. However, DFACA has yet to be tested for the full range of contingencies.

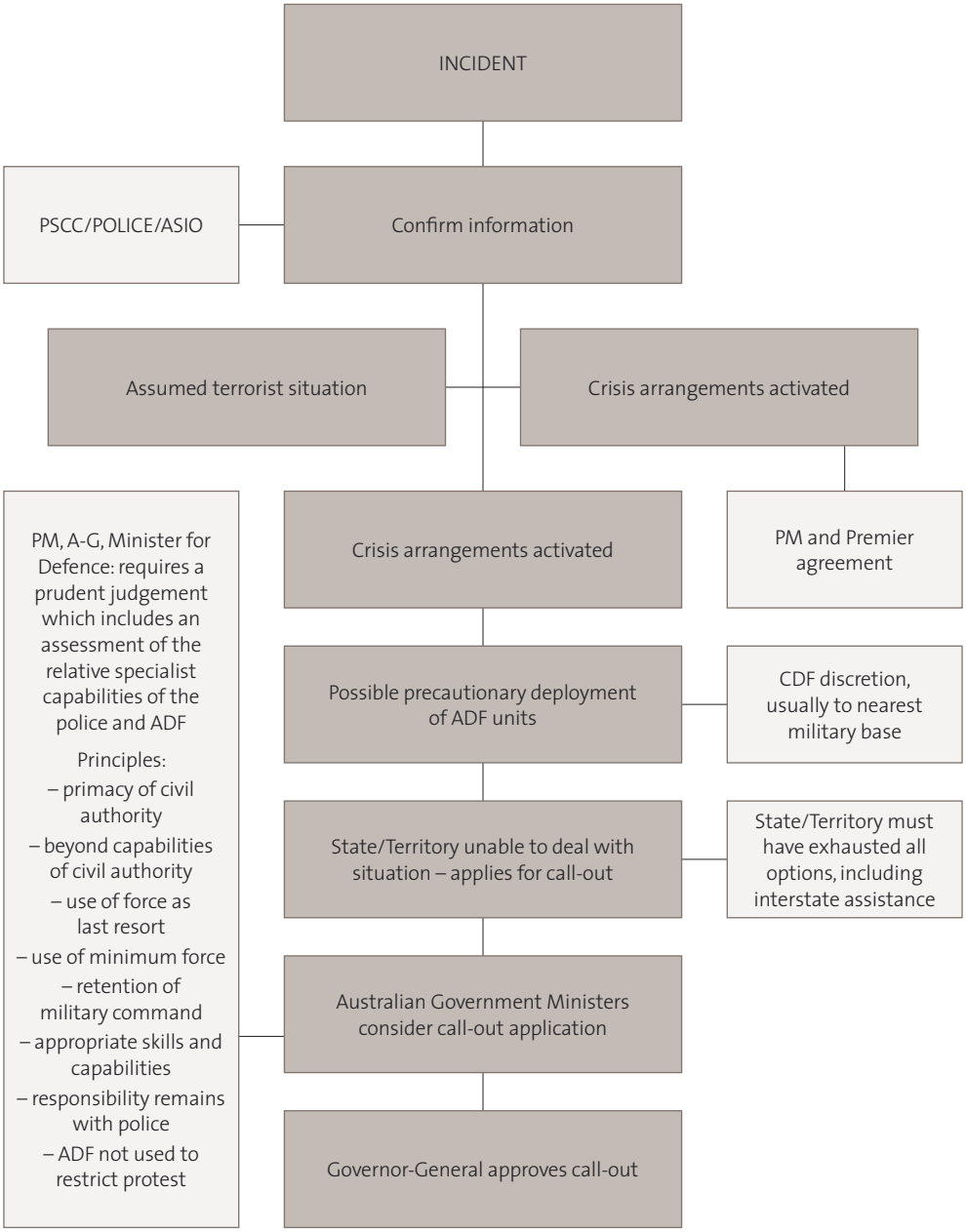
SAS troopers in Rigid Hull Inflatable Boat (RHIB) during Exercise Mercury, July 2004. © Defence Department

DFACA gives ADF members certain powers to search, recapture buildings, free hostages and seize dangerous things. Reserve forces may only be called out when the Minister for Defence, after consultation with the Chief of Defence Force, is satisfied that sufficient numbers of the permanent force aren't available.

The ADF can be called out when:

- domestic violence is occurring, or is likely to occur in Australia
- the state or territory isn't, or isn't likely to be, able to protect itself against domestic violence
- the state or territory isn't, or isn't likely to be, able to protect Commonwealth interests against domestic violence.

Figure 7: Call-out process under DFACA



Call-out of the ADF can be requested by a state or territory, or initiated by Australian Government if it believes the state or territory can't protect itself or Commonwealth interests. Figure 7 shows the call-out process.

DFACA only applies to onshore Defence counter-terrorism tasks. Until recently, for offshore terrorist incidents, the Commonwealth would exercise its executive power under section 61 of the Constitution to call out the ADF. In a major policy shift, the government announced on 15 December 2004 that the ADF, as part of its routine duties, would take direct responsibility for offshore counter-terrorism prevention, interdiction and response. No call-out will now be required.

In a major policy shift, the government announced on 15 December 2004 that the ADF, as part of its routine duties, would take direct responsibility for offshore counter-terrorism prevention, interdiction and response.

Control of naval waters

The *Control of Naval Waters Act 1918* provides for the protection of Defence land and/or installations used or owned by the Commonwealth, and empowers the Navy to prohibit, restrict or regulate any activity conducted within naval waters, in the airspace over these areas, or on their foreshores. Under the Act, Defence can exclude craft of any description and unwanted personnel. As with the MTSA security-level requirements for ports, the requirement to restrict non-defence activity within naval waters would vary with the level of threat and the use of the facility.

Naval waters can only be declared within a distance of five nautical miles from an installation, or two nautical miles from the limits of Defence land on which there's no installation. Naval waters are declared by an instrument of the Governor-General in Council. The main purpose is to ensure that naval operations are free from undue interference in those waters; the declaration doesn't confer ownership of these waters on the Navy.

Naval waters are a potentially useful vehicle that allows the Australian Government to assert jurisdiction in a port. It may be necessary to review existing naval waters and to assess possible new requirements for them around Defence infrastructure.

Naval bases and ships

Additional measures have been introduced to ensure the security of naval bases and ships. At home ports, naval fleet protection is largely handled through security subcontractors. Naval police provide limited sea-based patrols. Gangway staff of naval ships aren't armed when the ships are in Australian ports, although special security precautions are taken with public access on ship open days.

When RAN ships are in foreign ports, the level of force protection is based on a threat assessment by security agencies in Defence and other government agencies. The captain of the vessel dictates the actual steps to be put in place, so that the ship's response is tailored

to the threat environment of the port being visited. The Navy uses host-nation support for such measures as sea barriers, sentries at the wharf, picket boats and the arrest and detention of personnel. Liaison for host-nation support is conducted through the Australian embassy in the country to be visited..

There are minimum standards for security zones around naval vessels, but the exact distances are classified. In recent years, the Navy has been more ready to use powers under the Naval Waters Act. There are now inflatable markers at larger naval bases, marking the limits of naval waters. Foreign warships visiting Australia set their own security zones, factoring in Australian and their own threat assessments. However, this doesn't confer any ability to enforce those zones or confer immunity from Australian law should some event occur. Ports are also concerned about the additional costs imposed on port operations if the presence of a foreign warship leads to higher security risk levels that disrupt the routine operations of the port.

Ports have entered into arrangements with the RAN covering the interface between Navy vessels in commercial ports and port facilities, and the MTSA obligations of those entities. All naval ports comply with and usually exceed the requirements of the MTSA and the ISPS Code. Defence has a standard set of security measures under 'Safe Base' arrangements. Safe Base levels are an escalating set of security measures implemented to deal with increased threat levels.

A private company, Defence Maritime Services, is used to operate and maintain the Navy's fleet of harbour and patrol craft and for the routine patrol of naval waters. However, a significant gap exists in that landside and waterside contractors lack the capacity to respond to higher levels of threat or to an actual attack. These personnel are neither trained nor equipped for a counter-terrorism mission.

Passenger ferries

The MTSA covers passenger vessels on interstate voyages. The only passenger company in this business in Australia, TT Line (operating between Sydney, Melbourne and Tasmania), has introduced a number of security measures, such as screening cars and passengers passing through detectors and baggage checks. Current security procedures make it very difficult for an unauthorised person to board these ferries. The ship's integrity is protected by full-time security guards with an electronic verification system. Ship security officers undergo specific training, including in emergency procedures and drills. They're aware of procedures for dealing with any crime scene on board.

There's been liaison between the company and state police forces on emergency response, and police have completed a number of training sessions to ensure that they have the right techniques and equipment. However, less interaction has occurred with Defence. Security zones in port are in place for the ferries—25 metres at level 1, 50 metres at level 2 and 100 metres at level 3. Guards on board are unarmed but—given the response time in any emergency at sea—there's a strong case for arming them, perhaps with 'stun' weapons.

Cruise ships

An international passenger cruise ship is defined as one that has sleeping facilities for at least 100 people (other than crew members) and is being used to provide an international passenger sea transportation service. Under the Migration Act, cruise ship operators

now give DIMIA information on all people on board a vessel arriving from overseas forty-eight hours before the ship arrives.

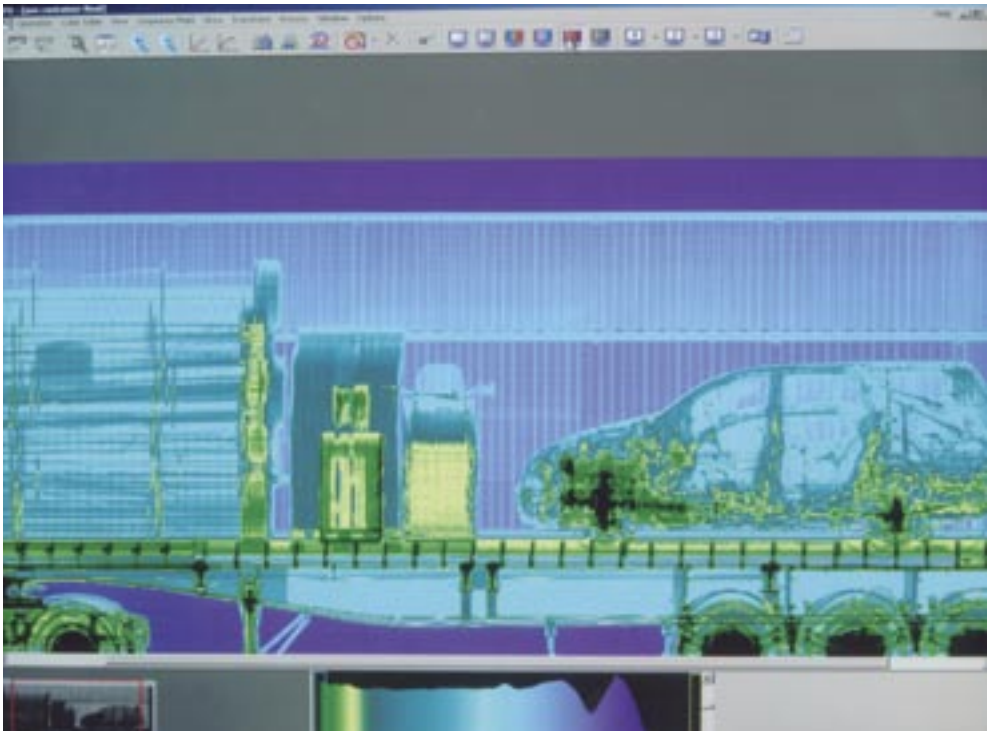
In December 2004, the US Congress approved tougher legislation requiring cruise lines to provide passenger and crew manifests before passengers embark on the vessel. The US cruise industry has objected that this will delay departures and inconvenience passengers while the government vets the passenger lists against its databases.

Container security

Considerable attention has been given in Australia to container security. The threat comes from our inability to know what's inside all of the three million shipping containers that cross Australian wharves each year. Customs has now opened four container examination facilities (CEFs) in Brisbane, Sydney, Melbourne and Fremantle, with a new facility to open in Port Adelaide in mid-2005.

Customs favours the CEFs, which use X-rays and other advanced search technologies, over mobile scanners, which are limited by lack of terminal space, transport congestion and smaller throughput. The X-ray operates within a purpose-designed building that incorporates the control room, image examination stations and ancillary functions. The CEFs integrate the container X-ray facility with a range of other technologies, such as pallet and mobile X-ray units, ionscan technology, detection dogs and radiation and chemical agent detectors. A large physical examination hall is part of the complex.

Search capabilities have been extended to deal with the full range of customs risks, including counter-terrorism. The aim is to prevent the flow of illicit drugs, weapons and prohibited goods into Australia, minimise revenue losses through smuggling and other forms of revenue evasion, increase the volume of sea cargo inspected, protect legitimate



Container x-ray imagery. © Australian Customs Service

industry from noncompliant importers and exporters through detection and deterrence, and improve sea cargo security. The CEFs serve much wider purposes than just preventing terrorist use of the container system, and it's misleading of government to identify CEF costs solely as counter-terrorist costs.

The units have already detected over $557.5 million of illicit drugs and have produced revenue benefits from the detection of alcohol and tobacco products. An adverse consequence of increased inspection rates has been some additional costs to industry—primarily storage fees.

Each CEF's target figure for X-ray inspection is based on the capacity of the technology and associated logistics requirements. A national target of 80,600 containers per year was established once the facilities were fully operational (26,000 containers each in Melbourne and Sydney, 15,600 in Brisbane and 13,000 in Fremantle). The July 2004 government commitment was to increase inspections from 80,000 to 100,000 containers (7% of the total of loaded import containers), which has now been achieved. The US inspects about 5.6% of containers; Canada inspects around 3%.

The choice of containers for X-ray is based on risk profiling of countries of origin, types of cargo, reliability of the importer and so on. Only around 10% of the X-rayed containers are then unpacked and physically examined. Very small numbers of exported containers are checked, and some bulk cargoes are tested.

It's highly probable that over time the proportion of containers X-rayed will be increased. The key, however, isn't in checking the most containers, but the right containers. Significantly increasing physical inspections isn't likely to result in appreciable national security benefits and could have adverse economic impacts.

It's highly probable that over time the proportion of containers X-rayed will be increased. The key, however, isn't in checking the most containers, but the right containers.

Personnel security

The Maritime Security Identification Card (MSIC) will be introduced during 2005 for employees in the maritime industry. This isn't a requirement of ISPS, although the US is introducing a broader Transportation Worker Identification Credential. Canada is introducing security clearance applications for transport workers. Other countries aren't implementing a maritime identity card, but many already have a national identity card.

There's currently no legislative requirement to check the background of people working in Australian ports and on Australian ships, but workers will need satisfactory background checks to acquire a Maritime Security Identification Card. The card is based on the aviation security identification card, although the two sectors are different.

The OTS will establish the regulatory standards and administrative processes for the scheme, but industry participants will be responsible for issuing, retrieving and disposing of cards.

ASIO, the AFP and DIMIA will do the background checking. Unlawful noncitizens and anyone with an adverse criminal history or security assessment won't get a card. It isn't clear if people who are already employed in the industry will be disadvantaged, if they have criminal records unrelated to terrorist activities. Applicants will be able to appeal to the Administrative Appeals Tribunal.

The aviation security identity card requires applicants to inform a potential employer of every conviction recorded against the applicant. The Maritime Union of Australia argues that any industry player who wants to introduce criminal background checks for their own purposes should do so by negotiations with the appropriate union and bear the costs. Maritime security, the union argues, should not be used as a cover to introduce other changes. There are proposals to protect current employees by 'grandfathering' certain criminal convictions, and through a spent conviction scheme that might apply to new employees.

Regional capacity-building

The OTS has been working on maritime security with countries in Southeast Asia and the South Pacific. It has posted liaison officers to Australian embassies in Manila and Jakarta to work on transport security capacity-building, and an OTS officer is working in Papua New Guinea on maritime security. The OTS works with Pacific island governments and the Pacific Community's Regional Maritime Program to raise awareness of transport security standards, increase compliance levels in the South Pacific, and assist the development of model maritime security legislation.

Customs has also provided some training for regional countries in customs intelligence, risk management and cargo profiling.

In the Philippines, DOTARS has established a port security project to improve the skills of port managers for implementation of the ISPS Code, and has run ISPS awareness workshops in Indonesia, the Philippines, Papua New Guinea, Thailand and Vietnam.

Five Power Defence Arrangement exercises have recently included counter-terrorism operations, but the arrangement isn't likely to take on a dedicated operational maritime counter-terrorism role.

Australia has worked on maritime interdiction exercises with Singapore and Japan as part of the Proliferation Security Initiative.

Risk assessment, intelligence and security levels

The OTS advises government on transport security in the maritime sector. DOTARS sets security levels for ports and ships based on intelligence advice and NCTC policy, working closely with ASIO and other intelligence agencies. ASIO performs threat assessments on the maritime sector, which guide the development of facility-level risk context statements. ASIO has had limited previous contact with the maritime sector, and is now placing liaison officers in Sydney and Melbourne to develop its knowledge of the industry.

Security assessments required by the ISPS process were commissioned by the ports and port facilities. The assessments identified existing security measures and procedures, infrastructure weaknesses (including human factors), key operations, risks to key operations,

and the likelihood and consequences of risk events. The assessments also selected measures to reduce levels of risk.

DOTARS took the view that it should be flexible about how ports, port facilities and ships develop security plans based on risk assessments. The department wanted the plans to be outcome based, with performance-based goals rather than prescriptive requirements. It then centrally reviewed port and ship security plans to ensure that all were evaluated using the same criteria.

The OTS plans to conduct continuing on-site compliance inspections and audits, but this is a significant challenge because there are few assessors with appropriate maritime experience. In the longer term, DOTARS will have to ensure that owners and operators continue implementing their plans.

The ISPS Code and its implementation in Australian law don't involve contingency response measures, but outline security requirements at IMO risk level 1, which is the default, low-risk level. IMO risk level 2 is a heightened risk for which external assistance may be required, and IMO level 3 is extreme risk, where a security incident is probable or imminent (at this level, the national counter-terrorism arrangements under the NCTP would be initiated). The security level creates a link between the ship and the port facility because it triggers appropriate security measures for both.

A move to IMO risk level 2 would be a major test for Australian ports. The heightened risk would require extra resources from the national and state governments, as well as a seamless interagency response, and would impose greater costs on industry.

Interagency coordination

Maritime Industry Security Consultative Forum

The Maritime Industry Security Consultative Forum (MISCF) had its inaugural meeting in August 2004 in Canberra. The forum is composed of key maritime industry officials and meets twice a year. It aims for a constructive exchange of views on high-level maritime security matters of an operational, legal, policy or regulatory nature, such as the implementation of the maritime security regime and changes to the regime. It also provides members with an opportunity to give the OTS feedback on its role as a maritime security regulator. In this way, members and the OTS can identify key issues for further consultation and policy development. The forum can set up working groups as needed.

The MISCF is considering the need to establish a separate maritime group in the Trusted Information Sharing Network, which is part of the Attorney-General Department's national Critical Infrastructure Protection (CIP) Program. The network is made up of an advisory council and various advisory groups. The advisory council is the main coordinating mechanism for the network, comprises business leaders and relevant government agencies, and has a direct link with the National Counter-Terrorism Committee.

The alternative to such a mechanism could be a DOTARS–MISCF agreement to use DOTARS websites to share transport-security guidance material and risk information. At this stage, maritime security hasn't engaged fully with the Attorney-General's critical infrastructure agenda. The connection will be important, because the CIP Program is doing most of the work on supply-chain security and the maritime sector needs to swap lessons with other sectors, such as energy.

One area that the MISCF hasn't yet examined is the development of a tailored counter-terrorism communications strategy for the maritime sector. This is a neglected area in the government's ongoing awareness campaign to protect Australians from terrorism.

... a tailored counter-terrorism communications strategy for the maritime sector ... is a neglected area in the government's ongoing awareness campaign to protect Australians from terrorism.

Port security committees

Port security committees have been established in all commercial ports. Their membership is wide, and includes police, Customs, industry representatives, service providers and emergency responders, as well as Defence in key naval ports. The committees are involved in the development of overall port security assessments and plans, and are working reasonably well as coordinating bodies. However, they appear to need guidance on the way ahead, including advice on the information they need to know (such as intelligence from national agencies, sensor data, shipping reports and supply-chain information) and are allowed to have. There's also a need for the port chief security officers and harbour masters to be security cleared so that there can be a seamless flow of information.

Because the MTSA applies to 'facilities' and not to 'ports', each facility (container wharf, gas terminal, oil installation, tug berth and so on) had to produce a plan. The plans were therefore developed independently, and this could lead to possible conflicting measures or overlaps that might jeopardise the efficiency of a port's response to a terrorist event. The Port of Melbourne, for example, has fifteen security plans. Security plans for individual port facilities are confidential to the industry participants. They aren't shared between facilities and don't get sent to relevant state agencies, even the Police. All this makes it difficult to develop a uniform command and control architecture for port security.

The port security committees lack a common format, procedure and training for sharing information across the various state, national and private sector stakeholders. They don't focus on the areas of ports that aren't security regulated beyond the ship–shore boundary, such as roads, bridges or tunnels that lead into the port—damage to which could disrupt the port. The large number of stakeholders increases the possibility of blind spots, with negative implications for overall strategy design, intelligence handling and responses to hostile events.

Most people who attend port security committee meetings are operational personnel, not security personnel. In the event of a contingency, they may not be able to fill a security planning and response role. This is very different from the situation in the aviation sector. Information sharing between port security authorities and police occurs more through strong interpersonal links than any set process.

The flow of intelligence to the committees appears rather haphazard. Current strategies for government information-sharing to industry participants are mainly web-based. There are several documents available on the OTS website that relate to risk assessment and a password-protected site for industry members that communicates information on a variety of topics. On the other hand, for industry-to-government communications, both routine and urgent, the OTS Operations Centre runs a 24-hour call centre to receive information.

Australian Maritime Defence Council

The Australian Maritime Defence Council is a non-statutory body chaired by the Deputy Chief of Navy and comprises around fifteen representatives from a range of maritime industry bodies and Defence. It meets twice a year and advises government on maritime issues in the area of national security. The council, which is a high-level but relatively informal forum, has addressed maritime security in recent meetings.

Naval control and guidance of shipping

The RAN maintains a specialist branch of maritime trade operations (MTO) officers drawn from the Naval Reserves, many with experience in maritime industry. The MTO Branch is designed to work with the maritime sector to control shipping in any defence emergency. The branch advises the Navy on a broad range of matters connected to the merchant marine and maritime trade, and on naval cooperation and guidance of shipping procedures. MTO officers work in ports, in the RAN and joint headquarters, liaising with shipping companies, ships' masters and port authorities. The branch is made up of around a hundred reservists. Officers are not based in all ports, but they seek information from all in order to get as complete a picture as possible of maritime traffic in Australia.

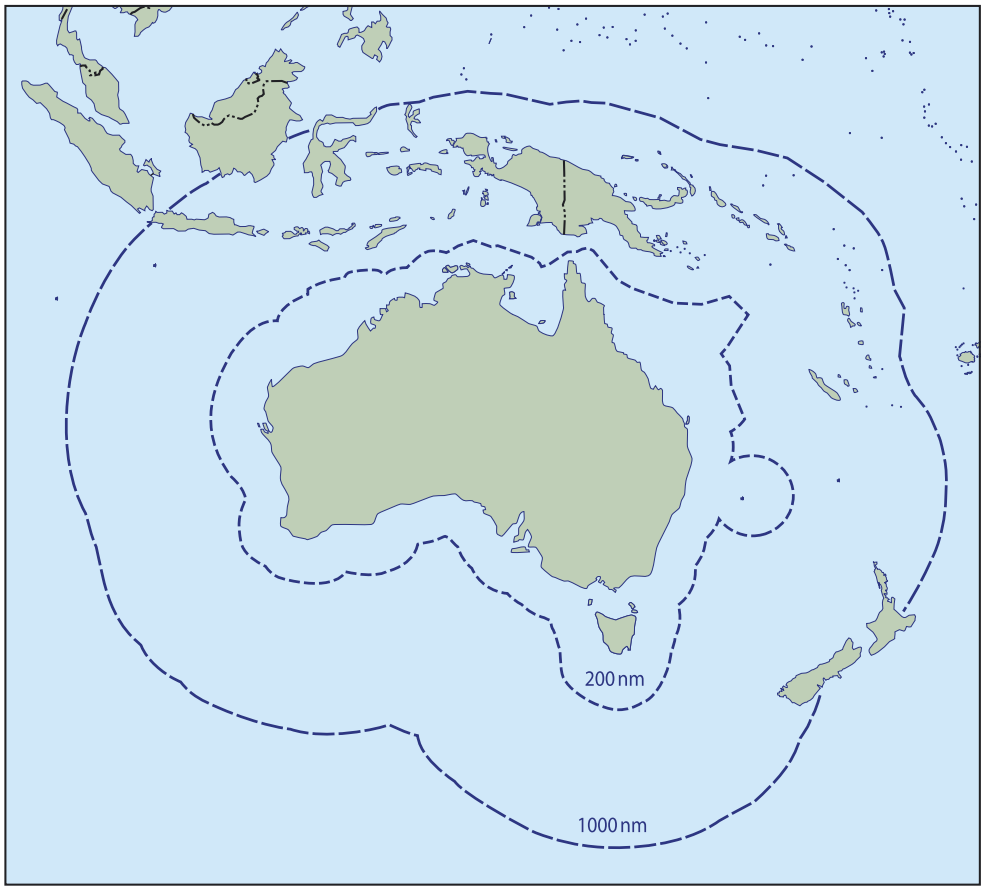
Joint Offshore Protection Command

On 15 December 2004, the Prime Minister announced that the Australian Government would assume direct responsibility for counter-terrorism prevention, interdiction and response in all offshore areas of Australia. This would allow the states and the Northern Territory to focus on initial incident response and security arrangements within ports. The ADF will take responsibility for offshore counter-terrorism prevention, interdiction and response capabilities, including the protection of offshore oil and gas facilities. Coastwatch will retain responsibility for civil maritime surveillance. The MTSA will be extended to apply to offshore oil and gas facilities.

Central to these new arrangements is a new Joint Offshore Protection Command established in March 2005. This command has a joint accountability structure, and is responsible to the Chief of Defence Force for its military functions and to the Chief Executive Officer of Customs for its civil functions. It is headed by the current Director-General of Coastwatch.

The new command will manage the Maritime Information System, which covers up to 1,000 nautical miles from Australia's coastline. On coming within this distance, vessels proposing to enter Australian ports will be required to provide comprehensive information, such as ship identity, crew, cargo, location, course, speed and intended port of arrival. Within Australia's exclusive economic zone, the aim will be to identify all vessels other than day recreational craft.

Figure 8: 1,000 nautical mile limit and 200 nautical mile EEZ (Exclusive Economic Zone) around Australia



Cartography by Jenny Sheehan

The challenges confronting the Joint Offshore Protection Command include data collection, the need for cultural change within the ADF and Customs to accept its role and authority, and target discrimination to identify threats. Even when the command has established an effective system for maritime domain awareness, threat identification and target discrimination will still be difficult and will likely require the interception and boarding of suspect vessels.

Dealing with operational incidents under the new offshore protection arrangements will require close consultation with those responsible for the NCTP, particularly in relation to long standing arrangements with state police and coroners. There's also work to be done at an international level to achieve cooperation from neighbouring countries, and to set up bilateral agreements to permit the boarding of foreign-flag vessels.


THINK
SAFETY

Chapter 5

WHERE ARE THE GAPS?

Introduction

Over the past two years, there have been sweeping changes in Australia's approach to maritime security, most notably the implementation of the MTSA. Australia has attached great importance to full compliance with the ISPS Code, and in some areas has gone beyond the code. There have also been significant advances in container security and personnel security.

Nevertheless, a number of areas of ship and port security need further attention. Achieving a consistent and coordinated national approach to the maritime terrorist threat is particularly pressing. Matters relating to foreign seafarers, interagency coordination, the role of Defence, training, research and development, regional capacity-building and supply-chain security also need further work. This chapter identifies the gaps and recommends measures to overcome them.

Achieving a consistent and coordinated national approach to the maritime terrorist threat is particularly pressing.

The management of high-consequence dangerous goods is a significant gap. These goods are a major vulnerability, requiring urgent attention to ensure nationwide consistency and to deal with potential risks. The Australian Government is currently working with the states and territories to develop a nationally consistent approach to security arrangements for the transport of these goods. This work must continue as a matter of high priority.

Photo opposite: Mooring hook. © APL

The national strategy to counter maritime terrorism requires extensive multidimensional approaches and close coordination between national and state agencies. Four distinct regimes might be identified as elements of the national strategy:

- a *legal and jurisdictional* regime that is, as far as possible, consistent across the Commonwealth, states and the Northern Territory, and includes effective legislation and supporting regulations
- a *protection* regime, including physical and personnel security arrangements, that implements international security measures for ships and ports and prevents illegal use of the maritime transportation system
- a *prevention and response* regime that provides effective operational measures to prevent terrorist attacks on ships and ports, and to respond to a maritime terrorist attack or the threat of such an attack
- a *cooperative, information-sharing and capacity-building* regime, involving relevant agencies and including institutional arrangements to ensure cooperation and information-sharing, as well as assistance to neighbouring countries in building their capacity for maritime security.

These four regimes together constitute the national capacity to counter maritime terrorism. Generally, good progress has been made with the protection regime but significant gaps exist in the other areas.

Legal and jurisdictional regime

Consistency is lacking

The interaction between state or territory legislation, and Commonwealth powers and responsibilities under the MTSA, Customs Act, Defence Act and other relevant Commonwealth legislation is complex. Extensive maritime assets, and many small ports, aren't security regulated under the MTSA, but all are state regulated through various state legislation and agencies covering public transport, dangerous goods, marine safety, pollution control, offshore work platforms, tourist facilities, recreational boating, commercial fishing or heritage protection. Some high-risk targets, particularly passenger and vehicle ferries, are solely under state jurisdiction—although it's likely that the Council of Australian Governments will conclude an intergovernmental agreement on surface-transport and mass-transit security that will cover intrastate passenger ferries. The capacity of the different states and the Northern Territory to deal with incidents in their jurisdictions varies greatly.

A great number of vessels that aren't subject to security regulation operate around the Australian coast, particularly fishing vessels, pleasure craft and yachts. This isn't to say that they should be regulated, but risk assessments should recognise the security problems created when these craft come into close contact with security-regulated vessels. Such contact might be with cruise liners in port or at anchor off tourist destinations, such as resorts and reefs on the Great Barrier Reef. Significantly, day recreational craft are excluded from the purview of the new Joint Offshore Protection Command, but they could pose a threat by covert rendezvous with other vessels.

The states and the Northern Territory are currently under considerable pressure from the Australian Government to increase their resource allocations to maritime security. There's a need for consistency in their responses. The state premiers and the Northern Territory

Chief Minister should jointly consider how they might coordinate capabilities in ports and offshore areas, achieve consistency of approach in maritime security, and contribute to the Joint Offshore Protection Command. This could include discussion of how the new command will interact during a maritime security incident with state emergency services, police, directors of public prosecutions and coroners.

Recommendation

The State Premiers and the Northern Territory Chief Minister should meet jointly to consider jurisdictional, legal, information-sharing and resource issues related to the coordination of capabilities to provide maritime security, including how the Joint Offshore Protection Command will interact with them in preventing and responding to maritime security threats or attacks. An illustrative statement that might emerge from such a meeting is included on page 7–9 of this paper.

Protection regime

Port protection

Landside port security is mainly undertaken by private security firms combined with physical measures such as boundary fences, controlled gates, cameras, alarm systems, guard dogs and so on. Training requirements for private security guards are set out in regulations, but the guards lack access to police resources and services, including key intelligence and law enforcement databases. They're transient workers, guarding a shopping mall one week and a port terminal the next. Port security is now too important to be dictated more by commercial considerations than by actual need. It's time to police the waterfront more thoroughly. For major ports, this requires specialised state port police, as exist at many US and European ports, with intimate knowledge of their maritime beat.

Port police would be key components of the intelligence and enforcement community responsible for port security. They'd be trained in all aspects of the new maritime legal regime. They would develop a high level of expertise for handling emergencies and would undertake patrols, investigate crime and advise port authorities on security and hazardous situations. They'd be able to provide operational support to other agencies such as DIMIA, DOTARS and Customs, and could be trained to undertake ship security boardings required

Security billboard. Photo courtesy Port of Brisbane Authority

by the MTSA. For '24/7' staffing, a police squad of around thirty would be required at each major port, with annual personnel costs of about $3 million. Capital costs for a control room, enquiry counter, radios, vehicles and so on would be about $800,000.

Recommendation

The states should establish dedicated port police units for major ports to work with state water police, and be responsible for port security on the landside.

Resources for port protection

The new port protection requirements of the MTSA are extensive, comprehensive and expensive, but no additional resources have been provided to the ports, port facilities and to state governments to meet them. The Australian Government view is that the port and port facility owners or operators are responsible for this funding, and that the extra costs are simply those of doing business. But the implementation costs to industry are estimated at $313 million in the first year, with ongoing annual costs of up to $96 million. So far, ports and the private sector have borne all the costs of additional port security. The funding the Australian Government has committed to port security has essentially gone to its own agencies, much of it for administrative costs, and not to the ports and port facilities.

The new port protection requirements of the MTSA are extensive, comprehensive and expensive, but no additional resources have been provided to the ports, port facilities and to state governments to meet them.

This approach contrasts with that in the US, where the government decided to help implement the ISPS by establishing a port grant program. To date, that program has provided the states with US$516 million in funds to support port security. The Canadian Government has also assisted ports directly through a $115-million program over three years. Joint funding arrangements for protective security at airports already exist in Australia—in 2004, the Australian Government committed $35 million in grants to regional airports to upgrade their security.

It's proposed that the Australian Government establish a $100-million Maritime and Port Security Program over three years, which could be directed towards port security projects. The funding should be on a cost-shared basis (80% government to 20% industry and port operators) for specified expenses in areas such as surveillance equipment, perimeter security, command and control equipment, and other infrastructure security measures such as water barriers. Each round of grants should be evaluated against a set of criteria specific to the round. Initial evaluation of grants should be undertaken at the state level, with final review in a national context by a specialist board chaired by DOTARS.

Recommendation

The Australian Government should introduce a $100-million Maritime and Port Security Program over three years, on a cost-shared basis, to further modernise and strengthen maritime and port security systems and programs.

Container security

Unlike the US, Australia doesn't demand particular forms of container seals. While we should move to refusing to accept a container without a security seal, we shouldn't get ahead of international standards for container seals and should work closely with the World Customs Organization (WCO) on standards.

Again, unlike the US, Australian ports don't employ 'sniffers' on cranes to detect explosive material in containers by monitoring emissions of heat and gas. This technology should be investigated for use here.

Electronic seal technologies aren't yet ready for commercial use. Rather than mandating the use of e-seals, DOTARS and Customs should place greater emphasis on the integrity of existing seals. Similarly, technologies are now available to track containers using sensors that can be built into the container. Customs and DOTARS should continue to actively monitor technical developments both in seals and in tracking devices, and engage within the WCO and the shipping industry on container security.

There's a need for information on the contents of a container before it arrives at an Australian port. The US has had a requirement since December 2002 that twenty-four hours advance notice should be given to US Customs before cargo destined for the US is loaded aboard a vessel at a foreign port. Australia should introduce a similar scheme, without which it's difficult to run a credible risk-based targeting program.

Currently, cargo vessels are required to provide a report of their cargo at least forty-eight hours before arriving in an Australian port. But 16% of cargo reports are reported late to Customs. While the container can't be moved until its contents have been reported to Customs, it isn't satisfactory that containers, potentially carrying dangerous goods, can enter Australian ports before Customs is aware of their contents. Without timely reporting, it's difficult to properly target container screening.

Around 700,000 empty containers are brought through Australian ports and cities each year to be stored until space can be found for them on ships returning to their ports of origin. Very few of these empty containers are inspected—the combined figure for the two financial years 2002–03 and 2003–04 was around 190. Customs should introduce a program of randomly inspecting transshipped empty containers, or of 'saturation' checking of empty containers in particular regions or wharves from time to time.

Recommendation

To strengthen container security, Australia should adopt the US 24-hour manifest rule for cargo destined for Australia and monitor developments in container seal and tracking technologies. Customs should also randomly inspect transshipped empty containers.

Supply-chain security

Security can't begin and end at the regulated security zone of a port, but must be integrated into the entire logistics supply chain. The security implications of the transport, packing and reporting of dangerous goods through the supply chain are assuming greater priority. This is where the real challenges will be in the future.

Ports are one node in the supply chain, and a ship is but a link between nodes. The best approach is one that looks at the supply chain in its totality. The security issues go across the supply chain for each consignment, from point of origin to point of destination. Many security concerns in the container transport chain are related to inland carriers and freight integrators—the first and last few links of the chain. Vulnerabilities in the container environment are highest in rail yards, road stops and shipping/loading terminals.

Supply-chain security requires the active participation of the logistics and transport industry to ensure that all parts of the container transport chain are included in a comprehensive security framework. Important work on infrastructure vulnerabilities across the supply chain is being undertaken by the Attorney-General's Critical Infrastructure Protection (CIP) Program. Some $12.5 million has been put into the CIP Branch for work on demonstrating dependencies and interdependencies in two CIP sectors: banking and finance, and communications. The roll-out to other sectors will be examined in the future.

Currently, no Australian Government agency 'owns' supply-chain security.

Currently, no Australian Government agency 'owns' supply-chain security. DOTARS focuses on some parts of the chain and Customs focuses on the border, while the Department of Foreign Affairs and Trade (DFAT) also has an interest, particularly in access into the US. DOTARS should be given the lead to work with Customs, DFAT and others to address the container transport chain in its entirety.

Recommendation

DOTARS should be given a clear mandate to secure the entire supply chain and work with Customs, DFAT and the Critical Infrastructure Protection Branch of the Attorney-General's Department to adopt a broader supply-chain security perspective that ensures port, ship and cargo security.

High-risk ships

Passenger ferries, cruise liners and US Navy vessels visiting Australian ports, as well as vessels carrying high-consequence dangerous goods such as ammonium nitrate, have been identified as high-risk ships. We need a nationwide approach to managing the security of such ships. Currently, the approach varies from state to state and occasionally even from port to port. The Australian Government must take the leading role and be prepared to

commit extra resources, including the routine involvement of the ADF, to ensure that the risk of an attack on these ships is reduced. At present, in some ports, commercial security contractors provide the security for these vessels, but appropriately armed and trained military or police personnel would be more effective. While classified guidelines have been developed, public confidence would be supported if an unclassified version were available.

Recommendation

The Australian Government, through the OTS, should develop publicly available guidelines for the security of high-risk ships in Australian ports, including for port visits by US Navy vessels.

Foreign seafarers

Since November 2003, DIMIA and Customs have been demanding passports, as well as seafarers' identification documents, from foreign seafarers. Face-to-face passport inspections are carried out by Customs for entry to Australia and shore leave. Customs undertakes primary immigration clearances on behalf of DIMIA, with around 80% (recently up from 70%) of crew being checked at first port of call. DIMIA provides secondary clearance, which includes responding to inadequately documented crew.

DIMIA is introducing mandatory electronic reporting of crew by shipping operators. Cargo vessels visiting Australia will be required to convey details of crew identity to DIMIA electronically forty-eight hours before arrival, and this may be changed to ninety-six hours. Under the Advanced Passenger and Crew Reporting System that applies to cruise ships, checks are made against an alert list to identify high-risk individuals. If no alert sounds, an electronic special purpose visa is automatically issued for the crew.

Customs may inspect the ship in port, but an international vessel can remain in Australia and carry out transport services along the coast under a continuing voyage permit (CVP) for up to three months. Two hundred and sixty CVPs have been issued since 2002, with 36 current at the time of writing; thirty-nine different vessels have obtained permits. There are strong grounds for requiring foreign crew who carry domestic cargo regularly between two or more Australian ports on a CVP over a three-month period, to be subject to the same checks as those on Australian crew members in ships entering Australia or operating in the coasting trade. The situation of foreign seafarers is somewhat different from that of foreign workers in other sectors of the Australian economy who work under skills shortages programs. Non-seafarers have to apply for a visa in advance, while seafarers are simply granted a special purpose visa on arrival in Australia if they possess a passport and a seafarer's identification document.

Recommendation

The Australian Government should conduct an investigation of the risks involved in the employment of large numbers of foreign seafarers on the Australian coast, including on vessels carrying high-consequence dangerous cargoes.

Prevention and response regime

State water police

The MTSA requires port operators to be responsible for waterside restriction zones within security-regulated ports, including areas under piers. Australian ports have few assets, beyond a small number of port service vessels in some ports for surveillance and monitoring of port areas, and no capacity for underwater surveillance. Defence is reluctant to be given security tasks inshore, and plays virtually no role in port security. Naval reservists have, however, assisted in an *ad hoc* fashion with clearance divers and mine countermeasures expertise. Port authorities have no capacity for minesweeping or clearance diving.

Existing waterside resources aren't adequate to effectively secure major and regional ports during higher levels of alert over an extended period.

Existing waterside resources aren't adequate to effectively secure major and regional ports during higher levels of alert over an extended period. Private security firms have limited maritime assets and lack training. The capabilities of water police are uneven across the state and territory jurisdictions, although other state agencies might also operate patrol craft. State-based marine police in some jurisdictions are being strengthened, but there's still limited water police presence in most Australian ports. Apart from NSW, no state has a capability to intercept and board vessels. Most state police forces have limited training and equipment, such as air and surface assets, for maritime counter-terrorism.

In November 2004, the NSW Government committed to a major $27-million overhaul of the state's water police, commissioning twenty-seven new vessels over the next four years.

NSW Water Police launch. Photo courtesy NSW Police

This will take the state's water patrol to about forty vessels based in seven ports. As well as Sydney Harbour and Botany Bay, the fleet will operate at Coffs Harbour, Eden, Port Stephens and Port Kembla. The flagship will be a $4-million, 30-metre vessel, and $2.65 million will be spent on a patrol boat that will be used for counter-terrorism operations.

NSW experience of the Olympics gave the state's water police extra resources. The Victorian police have fourteen vessels, but most of the other states are starting from a very low base.

The other states and the Northern Territory should follow the lead of NSW. Over the next four years, Queensland should commit $20 million, Victoria $18 million, Western Australia $18 million, South Australia $10 million, the Northern Territory and Tasmania each $5 million to provide for rapid-response and ocean patrol vessels, dive boats and surveillance craft to be used for counter-terrorism, crime-fighting, search and rescue, and guarding important maritime infrastructure.

To pay for an increased on-water presence at the ports, resources should be directed to state police forces from the dividends paid by ports to state governments. This transfer should be transparent and listed as a line item in state budgets. There should be no levy on ports to pay for extra water policing.

Recommendation

The states and the Northern Territory should strengthen security at major ports by upgrading their on-water capabilities.

Defence role

The ADF, while assisting water police with some training from time to time, hasn't wanted or sought a role in domestic security close to shore. However, the MTSA requires port response options at higher threat scenarios, possibly over extended periods. At higher levels, the ports would require external assistance, and in the absence of a coastguard the ADF that would be called on to render it. Aid from the ADF might be constrained by the legal requirements for call-out.

State resources are quite inadequate to respond to the higher threat levels associated with a terrorist threat or incident. This has been recognised in the US with the establishment by the US Coast Guard of mobile 'maritime safety and security teams', which provide protection for strategic shipping, high-interest vessels and critical infrastructure. They're a quick response force, equipped with armed fast boats, and are capable of rapid, nationwide deployment by air, ground or sea in response to changing threat conditions.

A rapid-response capability is already planned for regional airports in Australia, with the announcement by the Australian Government in early January 2005 of four regional rapid-response teams responsible for protecting 146 airports against terrorist threats. The teams, which will cost $20.7 million over five years, will be based at Melbourne, Sydney, Perth and Brisbane airports

The ADF should provide a maritime rapid-response capability similar to that in the US, with at least four Mobile Maritime Security Response Teams to be based in Sydney, Darwin and Townsville and at HMAS *Stirling*. These teams would also provide the capability for naval fleet protection at higher threat levels. They should be associated with the Navy's clearance

diving teams, and be able to respond to an underwater threat and clear mines. The RAN's Maritime Trade Operations Branch may be in a position to advise and support the teams.

The ADF should provide a maritime rapid-response capability similar to that in the US, with at least four mobile maritime security response teams ...

The Navy might also pre-position, at the major ports, mine warfare equipment, clearance diving gear, and small, well-armed and fast vessels. Defence should be involved in teaching counter-terrorism techniques both to water police and to maritime security guards, especially in interdiction management and the appropriate use of force.

Sea bed maps of ports (that is, mine-warfare pilot surveys) should be up to date. Navy clearance divers have a crucial role in comprehensively securing the ports.

This involvement by the ADF in port and harbour security should be recognised by giving formal responsibility for this task and for liaison with relevant national and state authorities to the appropriate operational commander. In the UK, the Flag Officer Scotland and Northern Ireland has a similar responsibility.

Such an arrangement will require a headquarters policy and contingency planning cell for port security. However, we stress that this responsibility is for providing a prevention and response capability for higher level threats, and not for the routine protection of ports and ships.

Recommendation

The ADF should have a direct involvement in providing security for ships, ports and port facilities against the threat of maritime terrorism. This responsibility should be assigned to the appropriate operational commander and include the establishment of Mobile Maritime Security Response Teams.

Maritime domain awareness

The objective of maritime domain awareness (MDA) is to identify and address potential seaborne threats long before they get close to Australia's shores—and we need it not only in our northern waters, but also in the south. MDA is an integrated approach to maritime security that ties in the threats of maritime terrorism, illegal immigration, drug smuggling, illegal fishing and marine pollution. It suggests the fundamental importance of having good information on which to base risk assessments and establish priorities for maritime security.

Getting comprehensive information about all relevant entities in Australia's ports and broader maritime domain and their respective activities is not merely a technological problem. Our approach must recognise all sources of data and information, and include intelligence that arrives long before a threat reaches port. Intelligence could range from non-specific threats against a particular port to a tip from a foreign port about the transport of dangerous material on a vessel.

Building a sea-situation picture to monitor maritime traffic approaching Australia that matches the picture available from air and satellite surveillance is a demanding task. We should build on existing surveillance and tracking assets, such as:

- the Australian Ship Reporting System (AUSREP), which is part of our maritime search and rescue system—the Navigation Act requires reporting by ships in the AUSREP area
- the Barrier Reef Ship Reporting System (REEFREP), which is the mandatory ship reporting system operating in the Torres Strait and the inner route of the Great Barrier Reef
- AIS, which is a broadcast system capable of sending and receiving ship information (identity, position, course, speed, cargo) to and from other ships, suitably equipped aircraft and shore—AIS can handle over 2,000 reports per minute and update information every two seconds, but has a short detection range
- voyage information from the Australian Maritime Safety Authority
- vessel-monitoring system data from the Australian Fisheries Management Authority and the Pacific Islands Forum Fisheries Agency.

Commercial sensitivities will apply to some of these data sources. Extensive information is also available from commercial sources, such as Lloyds and the Maritime Information Group, but at a price. A comprehensive long-range identification and tracking system for Australian waters may be many years away, although the IMO is currently looking to mandate long-range identification and tracking for SOLAS vessels.

MDA will be a responsibility of the new Joint Offshore Protection Command. It will require ongoing collaboration and cooperation between the national intelligence community and those in Customs, DOTARS and the private sector who have information on such things as manifest lists, bills of lading, crew lists and ship movements. A useful start has been made with the recent formation of a maritime security intelligence group for the timely sharing of maritime-threat intelligence between the intelligence agencies, Defence, DIMIA, DOTARS, Customs and Coastwatch. The development of comprehensive MDA is likely to require resources well beyond the additional cost of $4 million over four years currently allowed to manage the new 1000nm Maritime Information System.

Recommendation

The Joint Offshore Protection Command should give the highest priority to the development of effective maritime domain awareness, using all sources of relevant information.

Public awareness

While targeted information on the ISPS Code and MTSA has been given to industry stakeholders, there's been no focused effort to raise public awareness on maritime security risks. DOTARS, the National Security Division in the Department of the Prime Minister and Cabinet and industry peak bodies should collaborate to develop a strategy to communicate the risks of maritime terrorism and raise public awareness on maritime threats. Awareness-raising material could be provided to port authorities, waterside workers, fishers, yacht clubs, marinas, marine safety bodies and other groups for distribution. (See box on page 82 for an example of a possible awareness brochure.)

Recommendation

The government's campaign to raise public awareness about the risks of terrorism should include information to the community, especially the maritime community, on the risks of maritime terrorism.

Become a lifesaver—make Australia's seas and ports hostile places for terrorists

As someone who works on the waterfront, or who enjoys fishing, diving, boating and sailing or who just likes to watch ships come into port, you are a key member of the anti-terrorist squad.

Terrorists around the world have attacked maritime targets, including passenger and car ferries. The detonation of a large bomb at one of our major ports could cause significant loss of life and damage our economy.

One day, while enjoying our marine environment, you might spot suspicious behaviour—activity that just doesn't fit in—around piers, channels, ports, harbours, marinas, naval ships and bases, or at sea.

If you do see something suspicious, call the National Security Hotline on 1800 123 400. Our trained operators take every call seriously, and you can remain anonymous.

Your silence could be deadly.

Authorised by the Australian Government
—Working for a safer maritime Australia

Cooperation, information-sharing and capacity-building regime

Federal–state coordination

Each state has extensive and varied interactions in its maritime jurisdiction, which are in turn highly integrated with the state's transport and logistics infrastructure and hence with its economy. Many port facilities aren't within the security-regulated areas of ports. Each state's maritime security and emergency management 'canvas', with its interests in transport and public safety, is broader than the Australian Government's interest in the parts of ports and shipping that are regulated by the MTSA.

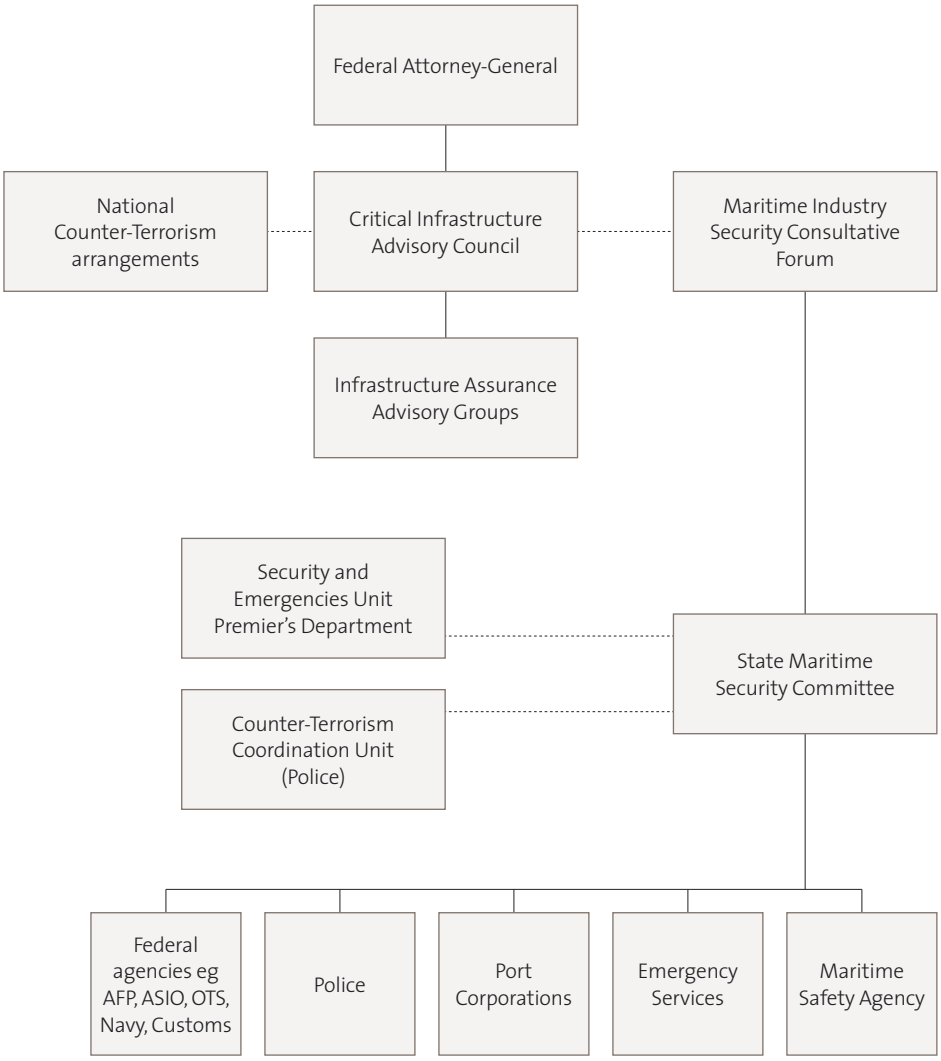
There's an absence at the state level of a single coordinating body that integrates and links maritime security across relevant national and state agencies, including port authorities. There are now joint AFP-led counter-terrorism teams comprising federal, state and territory police operating in all jurisdictions, focused on intelligence gathering, investigations and strategic planning, but their results aren't necessarily communicated to operators in the maritime sector.

There's an absence at the state level of a single coordinating body that integrates and links maritime security across relevant national and state agencies

Port security committees are focused on individual maritime security issues within their declared port areas, but aren't able to definitively extend their responsibilities across the supply chain by including other modes of transport. They don't link seamlessly with structures established at the state level on critical infrastructure protection, to the broader counter-terrorism architecture managed at the state level, or indeed to a substantial range of maritime and logistics interface systems.

State maritime security committees (see Figure 9) would help provide a foundation and framework to coordinate, integrate and develop common operational concepts and standards at security regulated ports, with their interrelated neighbours and stakeholders in

Figure 9: State maritime security committee



the state or territory, and with extensive state-regulated parts of the maritime environment. They should include members of state counter-terrorism bodies, major port authorities, police (including water and transit police), emergency services, maritime safety agencies, state transport and logistics agencies, and national authorities such as the OTS, Customs, AQIS, ASIO and the Navy.

Recommendation

State governments should establish state maritime security committees to develop, coordinate and integrate processes at security-regulated and other ports. The state committees would be the key components of a national maritime security architecture that links to the national-level Maritime Industry Security Consultative Forum.

Identifying major vulnerabilities

Data isn't currently available to allow a balanced assessment of the relative vulnerabilities of Australia's ports and shipping. Instead, Australia has adopted a general approach to maritime security that requires all ports, port facilities and ships to implement security measures under the MTSA, regardless of how vulnerable the asset might be. Some high-risk facilities, such as Coode Island in Melbourne, and high-risk ships have been identified, but otherwise ports, port facilities and ships conform to common requirements.

Australia has about 70 commercial ports, each with its own attributes and playing its particular role in the Australian economy. Clearly, some ports are more vulnerable than others. The relative impact on the Australian economy of the disruption of port activities will vary greatly from one port to another. The vulnerability of each port is a function of many factors, including how essential it might be to a particular trade, the economic importance of that trade, whether the trade could be readily rerouted to an alternative port, and how easily the port might be closed by terrorist action. The same might be said about the relative vulnerability of different ships carrying trade to and from Australia, or around the Australian coast.

The Bureau of Transport and Regional Economics has undertaken some work on the economic effects of a disruption to Australia's maritime trade. This type of work should be pursued to improve the quality of decision-making, leading to significant cost savings for both the public and private sectors, as well as ensuring that all the more vulnerable assets receive an appropriate level of protection.

Recommendation

The Australian Government should commission a comprehensive analytical study to identify key vulnerabilities of ports, port facilities and shipping.

Maritime skills

The Australian maritime sector has a real and genuine concern over a looming shortage of people with required seagoing qualifications. These maritime skills are needed in a wide range of areas, including ship management and ownership, towage and salvage services, maritime safety administration, pilotage, port and terminal operations, and now

in maritime security. The OTS has already had difficulty recruiting appropriately qualified people in its maritime security areas, and there may be longer term security implications if Australian industry can't find enough Australians with appropriate maritime skills to meet national requirements.

The maritime skills base in Australia is ageing, and there's a diminishing number of young persons being trained as seafarers in the Australian-controlled fleet. The situation is exacerbated by several factors, including the regulatory environment of the Australian shipping industry and differential tax treatment between Australians who are seafarers and other Australians working overseas.

Recommendation

The Australian Government should take action to reverse the current trend towards a declining maritime skills base, including through a sponsored cadet scheme to encourage young men and women to pursue a career at sea, and a review of the taxation regime for Australian seafarers working overseas.

Ship and port exercises

Realistic scenario-based maritime exercises should be held regularly so that port security leaders and government agencies fully appreciate the threats, risks and responses needed. To take one example, it isn't widely appreciated in the counter-terrorism community that there's a need to advise a harbour master, as well as police, of any maritime threat information. It's the harbour master who has to deal with the practical problems of responding to incidents, such as getting vessels out of a port at short notice.

Regular exercises are needed to test the ability of port leaders and sectors to detect and respond to a hostile attack, especially a multifaceted attack. Exercises often identify critical holes in contingency plans and serve to bolster relationships among key participants. They make the issues much less abstract for those who must sustain industry and government support for security resources. Several exercises at our major ports would test the current decision-making organisation at ports under stress, and test the capability of the command and control response. Defence should be involved in regular exercises with cruise ships and ferries, so that effective response options can be developed for these vulnerable maritime assets.

Regular exercises are needed to test the ability of port leaders and sectors to detect and respond to a hostile attack…

Recommendation

The Protective Security Coordination Centre, in cooperation with state police, port authorities and DOTARS, should initiate a regular round of confidential workshops for developing port security responses and maritime exercises to test port security leaders.

Scientific research

There's been no comprehensive investigation into the security research and development needs of the Australian maritime and port sectors. In July 2004, the Science, Engineering and Technology (SET) unit in the Department of the Prime Minister and Cabinet received funding of $7.2 million over four years for counter-terrorism research. In December 2003, the unit surveyed Australian, state and territory government agencies on counter-terrorism research and development. Maritime and transport agencies and industries weren't included. It isn't surprising, therefore, that the nine areas the SET unit identified for research don't focus on maritime security needs.

The SET unit and the Defence Science and Technology Organisation should develop greater understanding of potential research and development requirements to counter maritime terrorism. DOTARS should work with industry to fund maritime security projects with the SET unit on a dollar-for-dollar basis. Significantly greater funding through the unit for maritime security research and development is more likely in the future. Joint funding agreements are soon to be concluded between the SET unit and the US Technical Support Working Group, the US body that coordinates international research and development requirements for combating terrorism, and with the US Department of Homeland Security.

Recommendation

Australia's Chief Scientist should prepare a paper that addresses the scientific, technological and analytical requirements for Australian port and maritime security.

Regional capacity-building

Much is happening with maritime security in the Asia–Pacific region at present. APEC, the ASEAN Regional Forum and the Western Pacific Naval Symposium are all regional forums where maritime security issues are addressed. Defence, DOTARS and Customs have been undertaking programs in Southeast Asia and the South Pacific that assist capacity-building for maritime security. Customs has been attending meetings of regional coast guards, such as the Heads of Asian Coast Guard meetings, that deal with operational cooperation.

Japan has been actively using the Japan Coast Guard in Southeast Asian waters to help combat piracy and terrorism. Through the coast guard, Japan has been instrumental in establishing the Regional Cooperation Agreement on Anti-Piracy in Asia and the Asia Maritime Security Initiative 2004. The Japan Coast Guard is also assisting both Malaysia and Indonesia with the establishment of national coast guards.

Currently, Australia's regional maritime security responsibilities and capacity-building efforts are spread across several departments and agencies.

Networks of coast guard cooperation are developing in the region, at least partly in response to the threat of maritime terrorism. The increasing use of coast guards, rather than navies, for these cooperative activities arises from sensitivities about the involvement of navies. To the extent that Australia participates in these activities, it's through Customs—although Customs may not be the responsible Australian agency for many of the issues discussed.

Currently, Australia's regional maritime security responsibilities and capacity-building efforts are spread across several departments and agencies. Since September 2004, DFAT has been chairing an inter-departmental committee on regional maritime security cooperation to coordinate Australia's efforts in the region, including balanced assessments of priorities and exploration of the scope for cooperation with key regional players in regional maritime security, particularly the US and Japan.

Recommendation

The work of the inter-departmental committee on regional maritime security cooperation should be given high priority and sufficient funding provided to implement its proposals.

Chapter 6

CONCLUSIONS: TOWARDS A NATIONAL AND COORDINATED STRATEGY

The maritime terrorist threat

A terrorist attack on Australia's maritime interests is a credible scenario among the general terrorist threat contingencies facing Australia. We have high dependence on shipping and seaborne trade, and are adjacent to a region where terrorist groups have maritime capabilities. Targets might be identified by these groups as having strong iconic value to Australia, such as the Sydney Opera House and Sydney Harbour Bridge. All major Australian ports include facilities an attack on which could cause serious economic disruption, as well as loss of life where a facility is located in or near a centre of population.

... some of the more 'alarmist' maritime threats should be treated with scepticism.

However, some of the more 'alarmist' maritime threats should be treated with scepticism. In general, maritime targets are harder to attack than most onshore targets, including ones of iconic value and those where any attack would likely cause heavy loss of life, such as sports stadiums and urban mass-transit systems. Chapter 2 listed the more credible threats to Australia's maritime security. A possible attack on a cruise liner or passenger ferry, a vessel carrying high-consequence dangerous goods, or a US Navy vessel in an Australian port requires special attention in Australian contingency planning.

Photo opposite: Tugboat crew. © APL/Tom Stewart

There's always the risk of the maritime transportation system being used to smuggle terrorist personnel and/or materials into Australia, as well as the risk arising from the porous nature of Australia's maritime borders to illegal entry. Experience over the years with people smuggling and drug smuggling has demonstrated the problems involved in keeping our maritime approaches broadly secure. A determined and expert smuggler or terrorist is likely to have little difficulty entering Australia by sea, and will probably only be defeated by advance intelligence of his movements.

Some particular areas of Australia's maritime infrastructure warrant attention. These include offshore oil and gas facilities and LNG loading terminals in northwest Australia. This isn't so much because the risk of attack on these targets is high, but rather because defending them against attack, or responding to the threat of an attack on them, is so demanding of scarce resources.

The Australian response

The Australian Government, through the OTS, has been extremely energetic in putting in place appropriate legal regimes and protection measures to reduce the risks of a maritime terrorist threat. Since July 2004, the government has committed nearly $200 million to upgrading maritime security. Australia has comprehensively implemented the ISPS Code and has become a regional leader in other initiatives, including assistance to regional countries in building their capacity for maritime security and in developing and implementing new security measures through APEC and other regional associations.

The new maritime security environment has proven to have many advantages beyond a reduced risk of maritime terrorist attack. Increased inspection of incoming cargo reduces the risks of contraband smuggling generally, as well as the risks of cargo fraud and theft. The measures adopted to protect ports and maritime infrastructure make them more resilient not only to terrorist attacks but also to natural disasters or human error. The ports and shipping industries generally have welcomed the new measures, at least in principle. They recognise the benefits of the new security environment and have largely accepted the additional costs as part of doing business.

Chapter 2 identified two major challenges in meeting the risks of a maritime terrorist attack on Australia. These were institutional—to ensure coordination between the national and state agencies involved in maritime security, and operational—to meet the demands of geography and distance. Australia hasn't fully met these challenges. There's still work to be done, including building the national capacity to manage maritime security in the longer term.

Ongoing problems exist with coordination between national and state agencies, particularly as the states and the Northern Territory retain significant responsibilities in areas in which a threat from maritime terrorism is credible. The division of responsibility between the two levels of government is 'murky' in some respects, and states remain concerned about the flow of information and intelligence from Canberra. The establishment of state and territory maritime security committees would help overcome these problems.

While Australian ports and shipping have been strongly affected by the new maritime security environment, and the OTS is a powerful new player in maritime security, other government agencies are adopting a 'business as usual' approach. Australia has limited resources spread very thinly on the ground, and it's essential that all are mobilised against

the common threat. The new Joint Offshore Protection Command will be a major change in this regard, but Defence should also have a clear role in port and shipping security.

A whole-of-government approach?

A recent ASPI paper found that, while Australia has the NCTP and NCTC to respond to a terrorist threat, we have no whole-of-government, whole-of-nation strategy to fight terrorism on a comprehensive, ongoing and long-term basis (Borgu 2004). There had been a proliferation of counter-terrorism policies and strategies, particularly tactical or 'micro' responses (such as improved security legislation, increased funding to intelligence and law enforcement, more special forces, regional capacity-building measures and so on), but no overarching national counter-terrorism strategy.

... while Australia has the NCTP and NCTC to respond to a terrorist threat, we have no whole-of-government, whole-of-nation strategy to fight terrorism on a comprehensive, ongoing and long-term basis ...

This observation is apt in the maritime context. The NCTP notes, for example, that the jurisdictional responsibility for incidents involving ships at sea is determined by a number of circumstances and requires close liaison between potentially affected jurisdictions. This guidance appears to suggest a 'case-by-case' approach that will work against a quick and seamless response to a terrorist incident at sea but is no substitute for a comprehensive maritime security strategy.

Australia's Maritime Strategy

During 2003 and 2004, the Joint Standing Committee on Foreign Affairs, Defence and Trade (JCFADT) conducted an inquiry into Australia's Maritime Strategy with a view to determining the place of maritime strategy within Australia's broader military strategy and defence policy. Arguably this should have been within the context of Australia's broader *security* policy.

Somewhat surprisingly, the JCFADT's Report paid little attention to the risk of maritime terrorism and how it might influence maritime strategy. It noted the divergence between traditional Defence planning against conventional military threats, and a 'second position' with a 'new strategic agenda' encompassing regional instability, failing states, and the terrorist threat posed by non-state adversaries. While the Committee did not believe that it was a case of either/or between the two positions, it devoted most attention to conventional maritime security issues. DOTARS made a submission to the inquiry but this was focused on the place of merchant shipping in maritime strategy, particularly issues associated with the decreasing size of the Australian-flag merchant fleet. It did not address the pressing issues of 'maritime security' under consideration in the OTS. The Committee, therefore, missed an important opportunity to develop an overarching concept of maritime security and policy framework for Australia.

Whose maritime security are we talking about?

By expecting the maritime transport sector, including both private companies and state-owned ports, to bear the full costs of the new security measures, the Australian Government is treating these measures as though the benefits accrue only to the shipowner, or to the port or port facility operator. But it's the Australian community that is ultimately being protected from terrorist attack. At least in part, the new measures display many of the characteristics of a *public good* whose benefits are indivisible. If the measures are treated solely as *private goods* with benefits only for industry, then inevitably industry will tend to do the minimum amount required to ensure compliance with regulations.

A distinction can be drawn between the costs of the physical measures to protect a ship (the costs of meeting the requirements of the ISPS Code) or a port or port facility (the ISPS Code requirements, plus improved physical security through additional perimeter fencing, access controls, CCTV etc) and those of the operational measures needed to prevent or respond to a maritime terrorist attack. The former are the costs of doing business and should be carried mainly by the owner or operator of the ship or facility. However, the latter display more of the attributes of a public good. Their aim isn't to protect the ship or facility but rather to protect the community from a massive disaster. Their costs should be covered by government—either the Australian Government, or the state or territory government. This is no different from the Australian Government currently providing the resources to deal with a major chemical or biological attack.

Burden sharing

With state and local budgets haemorrhaging red ink, mayors, county commissioners, and governors are simply in no position to fill the security void the federal government has been keen to thrust upon them. The private sector has shown its preference for taking a minimalist approach to new security responsibilities.

(Stephen Flynn, *America the Vulnerable*, New York, Harper Collins Publishers, in cooperation with the Council on Foreign Relations, 2004, p 2)

In the final analysis, a patrol boat patrolling in Sydney or Darwin Harbour is no different from a warship patrolling further out to sea. Government is prepared to pay for the latter, so why not the former? If this principle is accepted, then it becomes a question of burden-sharing between the national and state governments. So far, and no doubt recognising that the states control all the major ports, the Australian Government has provided few, if any, additional resources for the prevention and response elements of maritime security in ports or close to shore. This situation has to change. To this end, we have recommended a meeting of the state premiers and the Chief Minister of the Northern Territory to discuss a coordinated position to take to the Prime Minister (see the illustrative statement on page 7–9 of this report).

As well as addressing burden sharing, this meeting would demonstrate the importance that our national leaders attach to maritime security, and confirm the need to enhance cooperation and coordination between the different levels of government. This would

ensure that our national resources for countering maritime terrorism are marshalled in the best possible manner, and that gaps in our maritime security are identified and remedial action taken.

It might well be questioned whether there is significant difference between meeting the threat of maritime terrorism and countering terrorism generally to justify a meeting of State Premiers and the Chief Minister of the Northern Territory, specifically on maritime security. However, this report has frequently pointed to the unique aspects of maritime security. These are due, not least of all, to the fundamental division of responsibility in the maritime domain between the state and federal governments. In many ways also, the types of threats faced by ports and ships are more varied and complex than those on land.

The Australian Government has put in place the national architecture to maintain maritime security, but much depends now on effective and consistent implementation by the states and territories. But currently the resources of the states and territories are quite insufficient to ensure that level of implementation, particularly as required to establish the necessary prevention and response regime for the higher levels of threat.

How much security is enough?

The basic problem in defence planning is determining how much defence is enough. Similarly, there's a challenge in providing security against the threat of maritime terrorism: finding the right balance between assessments of risk on the one hand and realistic costs on the other. And there must also be contingency arrangements to deal with higher levels of threat within the assessed warning time.

The basic problem in defence planning is determining how much defence is enough.

The OTS and ASIO have assessed that there's a terrorist threat to our shipping and ports, but it's clear that our resources are quite inadequate to deal with higher levels of threat that could arise with only a short warning. The additional resources committed by the Australian Government have largely gone towards enhancing the infrastructure of its own agencies. Industry and state and local authorities are being expected to provide much of the capacity to deal with and prevent higher levels of threat, while also meeting their basic protection requirements. This is an unsatisfactory approach. Assuming that the Commonwealth accepts its own risk assessments, it must then be prepared to accept a greater part of the financial burden in countering the threat.

It's normal practice for government departments to bid for more resources than the government budget can allow. In Defence, assessments of risk and warning time are tested by exhaustive analytical processes. However, there seems to be little testing of maritime security risk assessments and maritime counter-terrorism measures. They're simply asserted by the Commonwealth, and the private sector and state authorities are expected to comply. This situation is unsatisfactory. There's a need for greater transparency of the process to avoid excessive burdens being placed on industry and state governments.

Acronyms and abbreviations

AFMA	Australian Fisheries Management Authority
AFP	Australian Federal Police
AIS	automatic identification system
AMSA	Australian Maritime Safety Authority
APEC	Asia–Pacific Economic Cooperation
AQIS	Australian Quarantine and Inspection Service
ASIO	Australian Security Intelligence Organisation
CEF	container examination facility
CIP Program	Critical Infrastructure Protection Program
CSI	Container Security Initiative (US)
C–TPAT	Customs–Trade Partnership against Terrorism (US)
CVP	continuing voyage permit
DACC	Defence Assistance to the Civil Community
DFACA	Defence Force Aid to the Civil Authority
DFAT	Department of Foreign Affairs and Trade
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
DOTARS	Department of Transport and Regional Services
EMA	Emergency Management Australia
FPSOs	floating production, storage and offloading vessels
GBRMPA	Great Barrier Reef Marine Park Authority
IMO	International Maritime Organization
ISPS Code	International Ship and Port Facility Security Code

ISSC	International Ship Security Certificate
JI	Jemaah Islamiyah
LNG	liquid natural gas
LPG	liquefied petroleum gas
MDA	maritime domain awareness
MISCF	Maritime Industry Security Consultative Forum
MTO	Maritime Trade Operations (RAN)
MTSA	*Maritime Transport Security Act 2003*
NCTC	National Counter-Terrorism Committee (Australia)
NCTP	National Counter-Terrorism Plan (Australia)
OTS	Office of Transport Security (Australia)
PM&C	Department of the Prime Minister and Cabinet
PSCC	Protective Security Coordination Centre (Australia)
PSI	Proliferation Security Initiative
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RMSI	Regional Maritime Security Initiative
SAS	Special Air Service
SET	Science, Engineering and Technology unit of the Department of the Prime Minister and Cabinet
SIN	Ship Identification Number
SOLAS Convention	International Convention for the Safety of Life at Sea (1974)
STAR	Secure Trade in the APEC Region
SUA Convention	Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988)
SVP	single voyage permit
TEU	'twenty foot equivalent unit'; standard measure of containerised cargo
WCO	World Customs Organization
WMD	weapon of mass destruction

References and further reading

AAPMA (Association of Australian Ports and Marine Authorities Incorporated) (2005). Port Statistics. http://www.aapma.org.au/tradestats/

Australian Government (2004). *Transnational Terrorism: the Threat to Australia*. Canberra.

Berkenkopf K (2004). ISPS benefits doubtful, says German tramp owner. Lloyd's List online, 28 October.

Borgu A (2004). *Understanding Terrorism: 20 Basic Facts*. Strategic Insight 10, Australian Strategic Policy Institute.

DOTARS (Department of Transport and Regional Services) (2003). *Maritime Risk Context Statement*. Office of Transport Security, DOTARS, Canberra.

Flynn S (2004). *America the Vulnerable*. Harper Collins Publishers, New York, in cooperation with the Council on Foreign Relations.

JSCFADT (Joint Standing Committee on Foreign Affairs, Defence and Trade) (2004). *Australia's Maritime Strategy*. Canberra.

Richardson M (2004). *A Time Bomb for Global Trade*. Institute of Southeast Asian Studies, Singapore.

UPI (United Press International) 2004. Study models LNG terror attack. UPI, 21 December.

USN (United States Navy) (1993). OPNAV Instruction 5721.1E, dated 29 March 1993, Office of the Chief of Navy Operation, Department of the Navy.

Willis HH and Oritz DS (2004). *Evaluating the security of the global containerised supply chain*. Rand Corporation Technical Report.

About ASPI

The Australian Strategic Policy Institute (ASPI) is an independent, non-partisan policy institute. It has been set up by the Government to provide fresh ideas on Australia's defence and strategic policy choices. ASPI is charged with the task of informing the public on strategic and defence issues, generating new ideas for government, and fostering strategic expertise in Australia. It aims to help Australians understand the critical strategic choices which our country will face over the coming years, and will help Government make better-informed decisions.

For more information, visit ASPI's web site at www.aspi.org.au.

ASPI's Research Program

Each year ASPI will publish a number of policy reports on key issues facing Australian strategic and defence decision-makers. These reports will draw on work by external contributors.

Strategy: ASPI will publish up to 10 longer studies, including a series of annual publications on key topics, such as the defence budget, regional capabilities and Australian Defence Force capabilities.

Strategic Insights: A series of shorter studies on topical subjects that arise in public debate.

Commissioned Work: ASPI will undertake commissioned research for clients including the Australian Government, state governments, foreign governments and industry.

ASPI's Programs

There are four ASPI programs. They will produce publications and hold events including lectures, conferences and seminars around Australia, as well as dialogues on strategic issues with key regional countries. The programs are as follows.

Strategy and International Program: This program covers ASPI's work on Australia's international security environment, the development of

our higher strategic policy, our approach to new security challenges, and the management of our international defence relationships.

Operations and Capability Program: This program covers ASPI's work on the operational needs of the Australian Defence Force, the development of our defence capabilities, and the impact of new technology on our armed forces.

Budget and Management Program: This program covers the full range of questions concerning the delivery of capability, from financial issues and personnel management to acquisition and contracting out—issues that are central to the Government's policy responsibilities.

Outreach Program: One of the most important roles for ASPI is to involve the broader community in the debate of defence and security issues. The thrust of the activities will be to provide access to the issues and facts through a range of activities and publications.

ASPI Council Members

ASPI is governed by a Council of 12 members representing experience, expertise and excellence across a range of professions including business, academia, and the Defence Force. The Council includes nominees of the Prime Minister and the Leader of the Opposition.

Acting Chairman
Major General Adrian Clunies-Ross (Retired) AO, MBE

Members
The Honourable Jim Carlton AO
Dr Alan Dupont
Mr Michael L'Estrange
Mr Stephen Loosley
Mr Paul McClintock
Mr Des Moore
The Honourable Jocelyn Newman
Mr Ric Smith AO PSM
Brigadier Jim Wallace (Retired) AM
Dr J Roland Williams CBE

Director
Peter Abigail

Director of Programs
Peter Jennings

Operations and Capability Program Director
Aldo Borgu

Budget and Management Program Director
Dr Mark Thomson

Strategy and International Program Director
Dr Elsina Wainwright

Outreach Program Director/ Project Manager
Brendan McRandle

Research and Information Manager
Janice Johnson

Manager of Events and International Relationships
Lynne Grimsey

Office Manager
Jo Lo Presti

Information and Publications Officer
Paula Tychsen

Project Officer (Budget and Management)
Raspal Khosa

JOIN ASPI

Name

Position

Company/Organisation

❑ Government **❑ Non-Government**

Address

City **State** **Postcode**

Country

Telephone

Email

21139

SELECT 3 FREE PUBLICATIONS

❑ Your Defence Dollar: the 2004–2005 Defence Budget
❑ A Trillion Dollars and Counting: Paying for defence to 2050
❑ A Big Deal: Australia's future air combat capability
❑ Pay Your Money & Take Your Pick: Defence Spending Choices for Australia
❑ Sinews of War: the Defence Budget in 2003 and How We Got There
❑ Danger and Opportunity: Australia and the North Korea Crisis
❑ Our Failing Neighbour: Australia and the Future of Solomon Islands
❑ Building the Peace: Australia and the Future of Iraq

INDIVIDUAL	❑ 1 year *$199*	❑ 2 years *$378*	❑ 3 years *$537*
STUDENT*	❑ 1 year *$150*	❑ 2 years *$285*	❑ 3 years *$405*
INSTITUTION	❑ 1 year *$300*	❑ 2 years *$570*	❑ 3 years *$810*

* (STUDENT ID _____)

To subscribe
1) Mail to Level 2, Arts House, 40 Macquarie St, Barton ACT 2600, or
2) Subscribe online www.aspi.org.au
3) Phone (02) 6270 5100 or fax (02) 6273 9566

❑ Cheque ❑ Money Order ❑ Visa ❑ MasterCard ❑ AMEX ❑ Diners

Payable to Australian Strategic Policy Institute ABN 77 097 369 045

Name on card

Card no.

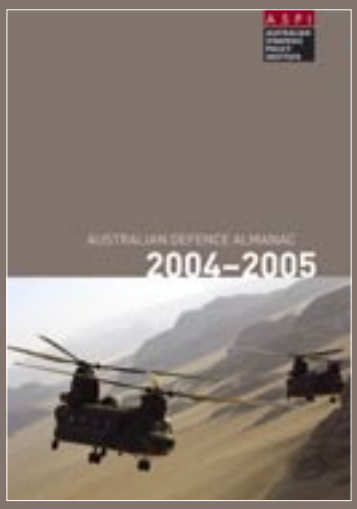
Expiry Date **/** **Total Amount $**

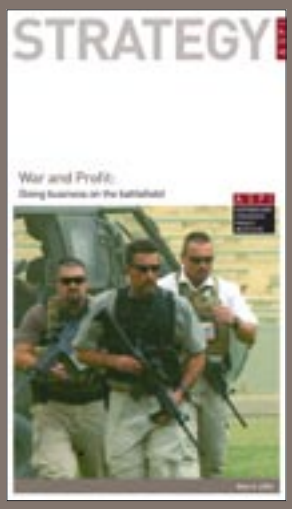
Signature

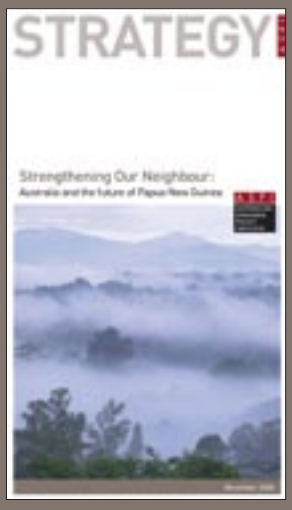
This will be a **TAX INVOICE** for GST purposes when fully completed and payment is made.

Please note specialist publications are not included.

Some previous ASPI publications







Future unknown:
The terrorist threat to Australian maritime security

The threat of maritime terrorism has led to fundamental changes in the international maritime security environment. There have been major developments in the regulation of international shipping, particularly through the introduction of the International Ship and Port Facility Security code. The Australian Government moved quickly to implement the code in Australia through the *Maritime Transport Security Act 2003* (MTSA), and to introduce a range of other maritime security measures, including additional facilities for screening containers and tighter immigration controls at seaports. The new measures have imposed large additional costs on the transport system and involved significant effort from both government and industry.

A terrorist attack on Australia's maritime interests is a credible scenario. We have high dependence on shipping and seaborne trade, and are adjacent to a region where terrorist groups have maritime capabilities. Australia still faces major institutional and operational challenges in reducing the risks of maritime terrorism. We haven't met these challenges fully, and we lack consistency in the response across the states and territories.

This report identifies where gaps exist in current arrangements. It includes recommendations to improve coordination between national and state agencies and to develop the national capacity to manage maritime security in the longer term. Other problem areas include the management of high-consequence dangerous goods, the management of the supply chain, and possible risks associated with the employment of large numbers of foreign seafarers on the Australian coast.

Although the Federal Government has dramatically increased spending on counter-terrorism measures, so far few, if any, additional resources have been provided for the prevention and response elements of maritime security in ports or close to shore. Several recommendations are made to redress this situation, including the establishment of a Maritime and Port Security Program, the strengthening of state water police, the establishment of state port police, and a specific role for the Australian Defence Force in ship and port security.

RRP $20.00

Z00 21139