

Refereed paper delivered at
Australian Political Studies Association Conference
6 – 9 July 2008
Hilton Hotel, Brisbane, Australia

Quandaries in Maritime Terrorism Policy

Michael Charles Buky B.A. (Hons)
University of the Sunshine Coast

Abstract:

An act of terrorism using a small vessel against commercial shipping or the ports they employ in Australia could have massive human and economic consequences. The Australian Government's approach to countering maritime terrorism has been incremental and slow to evolve but terrorists have demonstrated the capacity to adapt rapidly and outpace government policy. Counterterrorism policy in the maritime environment faces many challenges. Protecting vessels and maritime infrastructure against a potential attack is not only costly but difficult. Viewing maritime terrorism policy through the 'wicked problem' perspective assists in the formation of an innovative approach. The capacity of the Australian Government to act is limited by the need to comply with international maritime law and the requirement to negotiate with State Governments where jurisdictions overlap. This paper will consider the difficulty of implementing counterterrorism policies against the threat from small vessels to Australian maritime infrastructure. It will also argue that the current maritime security regime can be substantially improved.

Three separate maritime-related security incidents in Sydney Harbour alone have demonstrated the difficulty in preventing potential terrorists from reaching high risk targets. The highest profile security breach was the boarding of *HMAS Sydney* by two protesters in inflatable dinghies during its departure in 2003 for the Persian Gulf. The other two breaches concerned a small vessel that ran aground at Kirribilli point near the Prime Minister's residence in May 2007 and a swimmer in April 2008 who managed to enter the adjacent grounds of the Governor General's official home. The fact that these three incidents occurred within two miles¹ of each other in the country's premier harbour reveals the complexity of problems concerning the security environment in Australia's inshore and internal waters.

Despite an increased awareness of vulnerabilities in the maritime sector post-9/11, this paper argues that maritime terrorism presents a potential threat to Australian national security, its citizens and infrastructure. It also argues that the current protective regime does not take into account the considerable threat posed by small vessels.² This omission has occurred for a number of reasons. The first is due to a lack of recognition of the possible consequences of a successful attack. Another reason is the difficulty associated with establishing a national regulatory regime. Part of this difficulty stems from jurisdictional and legislative conflicts and responsibilities in a Federal system. The third and arguably the most important reason is the cultural change required within government to provide an integrated, innovative and comprehensive policy approach to the problem. These difficulties have resulted in a policy inertia regarding the small vessel threat. On the evidence of past terrorist attacks and threats globally, it is probable that State and Federal governments would react to any attack by enacting and implementing incremental measures to improve maritime security. This crisis-driven incremental cycle remains a feature of both anti-terrorist and counter-terrorist measures. When considering past examples, it is probable that terrorists will in turn devise new methods of circumventing prevention and interdiction in their own cycle of incrementalism. Breaking this cycle needs to be a priority of the Australian Government to achieve an improved maritime security regime. This policy quandary will be viewed through the 'wicked problem' framework and its requirement for an innovative approach.

From the policy making perspective, improving maritime security presents potentially unforeseeable and exceptional problems that are not amenable to the traditional linear, vertical and hierarchical approach that dominates the bureaucracy. In a recent paper the Australian Public Service Commission (APSC 2007, 11, 13, 21) identified the need for government to reconsider its approach to wicked problems admitting that such problems require holistic and innovative thinking to which the public service is unaccustomed. The APSC paper draws on and expands Rittel and Webber's analysis of wicked problems regarding planning theory in which 'social problems are never solved. At best they are only re-solved – over and over again (Rittel and Webber 1973, 162)'. An important element in the resolution of wicked problems that have trans-departmental responsibilities is the establishment of an overarching authority. With the plethora of

¹ All references to 'miles' refer to the nautical mile (nm) which is 1.15 statute miles or 1.85 kilometres.

² Reference to 'small vessels' refers to floating craft of less than 25 metres in overall length that are motor powered.

agencies and sub-agencies involved in maritime security, a coordinated and integrated response through one department would appear essential. This is supported by Bateman et al (2006, 119-142) who suggest that one minister be 'given responsibility for overall policy and legislative development in maritime enforcement and compliance' although they conclude this is unlikely to occur. The APSC (2007, 18) also recommends 'a dedicated Taskforce under strong leadership' reporting to 'the Prime Minister, a senior Minister or Cabinet committee' as a way of avoiding bureaucratic inertia. However, in the risk-averse public service sector, the required risk analysis followed by integrated and innovative policy making is mostly avoided in favour of incrementalism, even in time of crisis. Bateman et al (2006, 119-142) propose that the Australian Government approach to maritime enforcement and compliance may be termed 'crisis-driven incrementalism'. It is suggested that the term would be apt for government reaction to maritime terrorism and even for terrorism in general. In an area of acute concern such as national maritime security that impacts on the security of the state, it would be hoped that the required Taskforce be established before any crisis occurs. The APSC paper also emphasises that the inclusion of the people and communities affected in the policy making process is essential (2007, 27-29). This is especially important in the disparate boating community who are resistant to change, wary of petty incremental regulation and hard to police. Failure to engage the boating community's cooperation in any behavioural or regulatory change will jeopardise the resolution of this particularly wicked problem. However, such engagement is costly both in resources and time. With the budgetary cuts planned by the Rudd Government for 2008, it is doubtful whether there is sufficient will to establish the required processes for improved policy making in the maritime sphere. Breaking the cycle of incrementalism thus requires a changed policy approach that has so far not been demonstrated.

The security breaches in Sydney pale when considering Australia's 36 000km coastline, its 11 million sq km Exclusive Economic Zone (EEZ) and the state's near total economic dependence on sea-borne trade making it especially vulnerable to maritime threat. The logistics of monitoring, patrolling and securing vast sea areas that are crossed by large slow-moving commercial vessels, many of which carry high risk cargoes, present a substantial challenge. However, vessels within the 12 nm territorial sea and especially within internal waters are especially vulnerable. Their slow speed and difficulties in manoeuvring present ideal targets for fast small vessels. Ports and their storage facilities also present potential targets that are particularly vulnerable from the water. Acceptance of these vulnerabilities and that their protection rests within the sphere of a wicked policy problem lies at the heart of any resolution.

Although the Australian Government acknowledges that attacks are most likely to occur within these zones there is an absence in the public domain of analysis let alone policy documents on this vulnerability. Lachlan Payne, CEO of Shipping Australia, acknowledges that, '[a] ship navigating in confined waters or at sea is defenceless against any form of military-style attack' (2007, 12). In the target-rich maritime environment this suggests a level of vulnerability that has not been addressed by policy makers. If the vessels that carry 99.9% of the tonnage and 75% of the value of Australia's trade are

defenceless against such attack, this poses substantial questions concerning the state's physical and economic security (Truss 2005; Parliamentary Debates 2006, 55).

The economic and human consequences of an attack in a major port could be considerable. With an absence of economic projections in Australia, it is helpful to draw on examples from the US. Although Carafano (2007, 3) states that '[e]ven a large-scale disaster involving thousands of lives and billions of dollars in damage is unlikely to have long-term negative consequences for the U.S. economy', other sources disagree. For instance, a port security 'war game' in 2002 estimated that a nine-day nation-wide shutdown of US ports after a terrorist attack would cost \$74 billion.³ The Brookings Institute estimates that a successful attack with a nuclear, biological or chemical weapon could amount to \$1.3 trillion in lost trade alone (Bouchard 2005, 5). Since the value of Australian exports for the year ending September 2006 was \$152 billion (ABS 2006) with 99.9% of the tonnage carried by ship, this paper argues that any interruption to this trade could have a crippling effect on the Australian economy. Loss of confidence, insurance claims and stock market reversals during the current period of global economic volatility would magnify the cost considerably. Such an event could also have strategic implications by causing regional instability. It is therefore important to assess the likelihood of an attack.

Risk analysis assists in determining the need for more extensive measures to protect maritime infrastructure. The likelihood of an attack is an important component of this assessment. Government ministers and agencies have identified the terrorist threat to Australia many times. In 2003, the Australian Government acknowledged that the 'terrorist threat to Australians and Australian interests had increased, both domestically and overseas' (Department of Defence 2003). This threat was emphasised by the FBI's John Pistole, who stated that, '[a] terrorist attack on Australia was inevitable' (Sydney Morning Herald 2004). In the foreword to *Transnational Terrorism: The Threat To Australia*, then Foreign Minister, Alexander Downer writes of the 'grave threat now posed to Australia by international terrorism' while the document confirms unequivocally, 'Australia is a target' (Commonwealth of Australia 2004, v, vii). Former Director-General of ASIO, Dennis Richardson (2004, 25-26), confirmed that, 'al-Qaida [sic] had an active interest in carrying out a terrorist attack in Australia well before 11 September and ... we remain a target'. The current Director-General, Paul O'Sullivan, announced in 2005 that, 'ASIO currently assesses a terrorist attack on Australia as feasible and could well occur' (Todd 2005, 5). Although the Bali, Marriott Hotel and Jakarta Embassy bombings did not occur on the Australian mainland, they are concrete demonstrations of the threat against Australian interests. The continuing threat was re-emphasised in May 2007 by then Defence Minister Brendan Nelson who stated that terrorism 'has already shaped and will define much of our military security and other planning for the foreseeable future' (Dodd 2007, 6). Despite these statements, even if the likelihood of an attack is interpreted as 'unlikely' or 'rare' and it is accepted that the consequences of an attack could be 'major' or 'catastrophic', if applied to the matrix in Fig 1, the risk still remains 'high' or 'extreme'. This has profound implications for anti-terrorist and counter-terrorist policy as well as Australia's changing security role and the

³ All amounts are in Australian dollars converted at the rate of AUS\$1.25/US\$ 1

protection of its maritime trade. If the risk from an attack remains high or extreme, it is necessary to determine the ability of non-state actors to attack vessels and port infrastructure.

Fig 1 here

Several commentators have pointed to the The Liberation Tigers of Tamil Eelam (LTTE) as an example of a terrorist group able to maximise their maritime effectiveness with small vessels as their predominant platform. Gunaratna's (1998 in Raymond 2006, 239-257) suggestion pre-9/11 that the LTTE provide an 'early example of emerging trends and patterns in maritime terrorism' requires consideration. Drawing on the example of the LTTE, it is possible to assess the vulnerability of large vessels to small boats. Although the Sri Lankan Navy was on alert to the probability of attacks, since 1990 the Sea Tiger sub-group has carried out over 40 sea-based attacks, many successfully, against their vessels (Chalk 2002, 12). As well as having sunk the Sri Lankan Navy's largest warship, the *Sagarawardana* and captured its commander, the Sea Tigers also managed to disable nearly half of the navy's coastal patrol vessels (Rodeman 2003, 8). Michael Richardson (2004, 24) states that the Sri Lankan Government has lost 'at least a dozen ships' to explosive-laden high-speed small boats deployed by the Sea Tigers. Small vessels have thus proven to be highly effective in carrying out attacks against even well-armed and alerted naval ships. It is probable that this tactic was adopted and refined by al Qaeda when considering attacks against maritime targets.

The al Qaeda attack against the *USS Cole* in 2000 while in Yemeni waters further demonstrates the vulnerability of even well-armed vessels. Although the attack was unsophisticated in its use of a 'half-ton C4 platter charge', it resulted in the death of 17 sailors, injured another 42, nearly sank the vessel and caused \$375 million of damage that took 14 months to repair (TRADOC 2005, C-1; M Richardson 2004, 18). The success of this tactic demonstrates that small vessels provide a potent threat even to naval vessels in potentially hostile situations. Another example of a successful suicide operation was the 2002 attack by al Qaeda on the French tanker *Limburg*, also off Yemen, using a small boat. This attack killed one crew member and started a potentially devastating fire. After the attack, the International Maritime Bureau confirmed that,

[n]o shipboard response or action can protect the ship in these circumstances ...
Post-Limburg, we cannot continue to hope for the best and ignore the lessons
(Abhyankar 2002, 13).

Attacks against defenceless hydrocarbon tankers provide the potential not only for large loss of life but profound economic consequences.

It is important to consider the value of an oil tanker and its cargo. The world's largest oil tanker, the *Knock Nevis*, carries four million barrels currently valued at \$500 million⁴, while the vessel itself may be worth \$150m. If such a vessel were attacked in a port, consequential loss including human, clean-up and infrastructure damage costs would multiply these figures many times. Bearing in mind that the clean-up costs for the the

⁴ At a cost of US\$100 per barrel.

1989 *Exxon Valdez* oil spill amounted to over \$4 billion with further compensation of \$3 billion being considered by the Supreme Court twenty years later (Barnes 2008), estimating the total possible cost of a terrorist incident becomes problematic.

These vulnerabilities are further demonstrated with the failure to protect even high security events and zones. In Australia, the departure of *HMAS Sydney* from Garden Island naval base in 2003 for the Middle East was delayed by protesters in inflatables who boarded the bow and stern of the vessel (AAP 2003). This event demonstrated the vulnerability of large, hard-to-maneuvre vessels while transiting confined waters. Although the small craft that came alongside the vessel only carried protesters, it also demonstrated the ease with which terrorists could have mounted an attack. In 2007, Greenpeace activists succeeded in painting a message on an anchored bulk coal carrier in Newcastle. Although such vessels are not classified as high risk, the number at anchor and their hull value would provide easy and rewarding targets. These instances not only confirm the vulnerability of large vessels and the ability of small vessels to mount a successful 'attack', but also many quandaries for the policy maker.

At the entrance to the Suez Canal on 25 March this year, a vessel under contract to the US Navy fired a warning flare then warning shots at a small vessel heading towards them, killing one crew and injuring two others (BBC 2008). Failure to address the interface between large and small vessels in confined waters could lead to greater distrust and more such instances. As small vessels frequently abound in port and transit areas, this problem needs resolution. The regulation of small vessels and their identification while underway are measures that would meet many security requirements.

Security concerns also revolve around innovations in weaponry. A component of asymmetric warfare is the incremental use of technology and innovation by both counter-terrorist and terrorist operatives. As one avenue for attack closes, the terrorist is obliged to find alternative means and targets. Hoffman notes this with IRA attacks during the 'troubles'. When the British military detected a new technology for explosive detonation, they immediately enacted counter-measures. These measures were then countered by the IRA which subsequently developed new devices, frequently managing to stay a step ahead of the army (Hoffman 1998, 180-182). Lest it be thought that the IRA were in any way amateurish, their devices and detonators received begrudged admiration from those intent on their interdiction. A staff officer from the British army's 321 Explosive and Ordnance Disposal Company commented, '[w]e are dealing with the first division ... We have a great deal of respect for their skills' (Gorman 1992). In America, Secretary of Defence, Robert Gates, admitted similar concerns in a 2007 Congressional hearing, 'We find one way of trying to thwart their efforts — they [Iraqi insurgents] find a technology or a new way of going about their business' (Yaukey 2007). It is of concern that innovation and new technologies are now shared more easily and rapidly than ever before through globalised communications enabling a rapid incremental terrorist response. However, the equivalent counter-terrorist response may be hampered by the vertically and hierarchically structured bureaucracies of government. When new policy has to be coordinated by a plethora of departments and agencies, there will be inevitable delays, jurisdictional disputes and a fractured response to innovation in weaponry.

Incrementalism applies not only to the terrorist who is attempting to evade new security methods but also to government policy, legislation and counter-terrorism activities. The reactive and incremental nature of anti-terrorist legislation and counter-terrorism provisions can be demonstrated by current policies and procedures. The restrictions on liquids in aircraft passengers' hand luggage stems directly from the alleged plot of August 2006 in the UK to make explosives aboard by combining liquid components. Innovation by terrorists is a form of incrementalism that is driven by the 'crisis' of communications being intercepted or devices being detected or jammed before their detonation. It thus appears that both sides are engaged in incremental changes to their methods, policies and tactics. These incremental changes suggest that any method may be used to escalate damage and casualties, as well as their prevention. Western Governments that are obliged to observe many restrictions in their fight against terrorism as well as needing to placate a public that is resistant to draconian security measures may thus be outflanked by terrorists who have few, if any, compunctions. Breaking the cycle of bureaucratic incrementalism thus requires an appreciation of, and an adaptation to, terrorists' incrementalism and their organisational structures.

Incrementalism can also be applied to the munitions and tactics deployed. The terrorist use of small vessels fitted with innovative weapons and technology could represent an incremental change in tactics with far-reaching consequences. Innovation can result from the revival of old technologies to enable major incremental changes. For instance, an Improvised Explosive Devices (IED) is a weapon that relies solely on explosives without a directional component. However, a shaped charge uses a smaller amount of explosive while its force is directed to great effect. Shaped charges are not a recent innovation. In the 1880s Charles Munro noted that the detonation of a high explosive with a cavity facing the target left an indentation. This eventually led to the use of shaped charges in both surface and sub-surface demolition work as well as in munitions such as the modern TOW anti-tank missile. The platter charge that proved to be highly effective in the *Cole* attack is an unsophisticated form of shaped charge that focused and directed the explosion. The Explosively Formed Penetrator (EFP) is a refinement of the shaped charge. The principle behind the EFP is the use of a relatively small explosive charge in a steel cylinder closed at one end and with a machined concave copper cap pressed into the open end. When detonated, a slug of molten copper is expelled at high velocity towards the target. This slug is able to penetrate the depleted uranium armour used by the 60 ton Abrams tank.

The US Government response to this innovative use by insurgents in Iraq has been slow and expensive. Despite an annual budget of \$5 billion, the Pentagon has failed to equip the military with Mine Resistant Ambush Protected (MRAP) vehicles (Eisler et al 2007). Although MRAP vehicle design was developed in South Africa in the 1970s, the failure to deploy them appears to lie in the bureaucratic confusion surrounding repeated government statements that victory in the Iraq war was imminent. Furthermore, this available low-tech and relatively expensive approach did not reflect the high-tech problem solving capacity of the Pentagon-run Joint IED Defeat Organization. Hence,

even a large budget to resolve the wicked problem of EFPs failed to provide a short term but pragmatic approach in the face of bureaucratic dysfunction.

EFPs are still being used to great effect against US armoured vehicles in Iraq. Their migration to other spheres of terrorist operation is a probability with a potential wide range of applications. A video of an EFP measuring approximately 150cm long by 5cm diameter shows detonation making a large hole in a 10 cm steel plate, then penetrate a further 100 cm into the ground (Discovery Channel). The stated range is 100 metres. The potential use of EFPs mounted on small craft would present a substantial threat in the maritime environment. For example, their deployment on jet skis that are capable of 40 knots would present a threat of unimaginable magnitude. It is therefore essential to evaluate the vulnerability of targets to such devices and, above all, those that have the highest consequential damage potential. An EFP deployed against a LNG tanker could cause devastating consequences although the escaping supercooled gas would need separate ignition. Shore side facilities, where LNG is stored in a gaseous state, are even more vulnerable. Deployed against a crude oil tanker, an EFP could ignite the cargo, cause the vessel to founder and initiate a costly pollution event. As the US military acknowledges that terrorist attacks will continue by diverse actors against state interests globally for the foreseeable future, it is probable that terrorists will develop further devices that are deployed in new ways and to great effect in all spheres of operation.

Another quandary for policy makers is to determine the degree of regulation required that not only reduces the likelihood of an attack but also that which is acceptable to the boating community. Floating patrols inshore that check boat registration and operator licensing may have some effect but these are by nature irregular, widely dispersed and costly to run in both personnel and equipment. Another method to consider is the implementation of exclusion zones around vessels during different stages of their voyage. These could be based around the 500m radius exclusion zone stipulated in the *Maritime Transport and Offshore Facilities Security Act 2003* around all offshore installations. However, even if this exclusion zone were implemented for large vessels underway, and its enforcement was possible, it would still provide little protection. Evasive or other measures are impossible in the 50 second transit time to its target that a small vessel travelling at 20 knots would require, although the crew may at least be alerted. It must be questioned what measures a large vessel can take even with a longer warning. In ports and port approaches, enforcement of such a zone becomes problematic owing to the nature of the confined waters and the plethora of other craft in the vicinity. Many Australian ports use exclusion zones but their radius, the occasions on which, the areas to which, and the class of vessels around which they apply appear to rely on each port's discretion. For example the Tasmanian Government has implemented a permanent '50m exclusion zone around passenger ships, warships and tankers' whether underway or berthed in the port of Hobart (MAST 2007). Although the Port of Brisbane may implement exclusion zones, these depend on the type of vessel and cargo, its status (whether it is berthed or under way) and current security alerts.⁵ A senior pilot with the Port of Brisbane states that the only permanent exclusion zone of one mile radius is for

⁵ Pers. comm., Brisbane Port Security, 15 November 2007.

nuclear-powered or nuclear weapon carrying vessels ie US Navy ships.⁶ The Port of Melbourne (Victorian Notices To Mariners 2005) enforces 'waterside restricted zones' for some piers and docks while the Sydney Ports stipulates restricted zones around cruise ships and tankers only while berthed.⁷ Despite both Sydney and Melbourne experiencing a high level of large and, above all, small vessel movements, they have not implemented any permanent exclusion zones for vessels underway. Furthermore, even with a substantial increase in resources the effectiveness of such exclusion zones is questionable owing to the difficulty of enforcement in high density traffic areas. These examples also illustrate the uneven nature of security enforcement within a federal system while simultaneously permitting a degree of port autonomy based on risk assessment.

A passive system reinforced by patrolling vessels would be not only more cost-effective but more effective overall. Such a system is available through the fitting of an Automatic Identification System (AIS) transponder to every vessel over a certain length and engine kilowatt rating. The AIS signal can be transmitted via satellite to provide a comprehensive local picture of all vessels. AIS is currently mandatory only for SOLAS vessels⁸ and transmits information on vessel size, speed, course as well as the destination and cargo. A vessel monitored on radar that fails to transmit an AIS signal would be immediately investigated.

AIS regulation would require substantial cooperation between the States, Territories and Federal Government as well as between their respective departments. The need for a whole of government approach for such wicked problems is confirmed in the ASPC policy document (ASPC 2007, 4, 20). Currently, the States and Territories regulate small vessels regarding registration, anchoring, mooring, on-board safety equipment and requirements for operator licensing. Registered vessels are required to carry their registration number on the hull. States also have police and other emergency offshore responsibilities. However, it should be noted that the implementation of these responsibilities is not clear. For example, the Caloundra Fire Service on Queensland's Sunshine Coast has responsibility for fires on commercial ships using the channel close offshore that leads to the Port of Brisbane. They train for such events using hull mock-ups on land and simulated fires on vessels afloat. However, there is no dedicated vessel to transport fire fighters and their equipment to a vessel requiring assistance.⁹ States also enforce speed restrictions, blood alcohol levels and the wearing of lifejackets when required by legislation. Although each State and Territory has its own anti-terrorist legislation, none has legislation specifically relating to maritime terrorism. Furthermore, States and Territories appear willing to allow the Commonwealth to take over jurisdictional and operational control in a terrorist incident. Indeed, it would be hard to imagine the Federal Government not becoming immediately involved in any terrorist incident, let alone an attack against maritime infrastructure. It would thus appear that the

⁶ Pers. comm., Brisbane Pilot, 10 April 2008.

⁷ Pers. comm., R. Heath, Sydney Ports, Navigation Services Manager, 15 November 2007.

⁸ Safety of Life at Sea Convention (SOLAS) requirements apply to ships over 500 tonnes gross and passenger vessels on international voyages. In December 2000, SOLAS was amended to require the installation of AIS on all vessels over 300 tonnes built after July 2002 and engaged in international voyages.

⁹ Pers. comm. Queensland Fire Service, March 2008.

States' role in any future regulative changes regarding small vessels will be the broadening and enforcement of their existing responsibilities. This leaves a marginal role for the States in terrorist matters in which, after a primary response, they would complement the federal agencies and the Australian Defence Force. Following federal involvement, political issues regarding jurisdiction may surface, particularly if the outcome of an intervention is unsuccessful. This uncoordinated and fragmented approach portrays the failure in establishing an integrated maritime security policy. There are also concerns regarding conventions and legislation as well as to the class of vessels and zones which they apply.

The Australian Government has been active in the international and national arena regarding the drafting, implementation and enforcement of international conventions designed to improved maritime security. However, vessels under 500 tonnes, which are excluded from international conventions, are also omitted from any national legislation or regulation. It is of concern that the class of vessels most likely to be involved in a maritime terrorist incident has no security regulation whatsoever. Although such amendments would require international agreement, the regulation of Australian registered vessels on a passage through its territorial sea is within the Commonwealth's jurisdiction. While States maintain jurisdiction up to 3nm from the territorial sea baseline, and in some cases 12nm, the increasing control of the Commonwealth in maritime security issues would suggest that agreement could be reached with the States and Territories regarding security changes that would cover all vessels in the territorial sea. Although this would lead to a regulative disparity between Australian and foreign registered vessels, it would also serve as a model that could prompt amendments to international conventions that have failed to keep pace with the post-9/11 security regime.

The *HMAS Sydney* incident when exiting Garden Island in Sydney Harbour provided a vivid example of the inability of the Australian authorities to protect a capital ship in the country's major port within a densely populated urban area. If the authorities and the crew of the *Sydney* are unable to protect such a vessel in confined waters, it is doubtful whether they are able to protect the numerous cargo vessels that have substantially greater vulnerability when transiting the territorial sea and beyond.

Even if the Commonwealth were to obtain overall control of maritime security, it is far from clear how implementation would be achieved using current government structures. With 'at least 12 Commonwealth agencies with an ongoing role in maritime enforcement and compliance' (Bateman et al 2006, 119-142), inevitably there are operational and jurisdictional differences that could cause confusion and inadequate performance in the event of a terrorist incident. For a timely, reliable and effective response, integration of the many agencies and sub-agencies into a single authority for the administration of a comprehensive maritime security policy would appear essential. Agency systems would also benefit from integration. For example, harmonisation of computer systems should be a priority. Without a single authority to implement maritime security policy, it is hard to imagine how the proposed AIS system, or any other system, could function effectively. Forming a holistic, cohesive, integrated and uniform national policy within the current

bureaucratic structure would appear problematic in the extreme. If it is accepted that, in the context of a wicked policy problem, the improvement of maritime security is a necessity, organisational restructuring to enable the optimum policy making model becomes equally essential. It may be anticipated that as this institutional change is anathema to the traditional bureaucratic model it would be strongly resisted.

In May 2007, terrorism specialist, Bruce Hoffman, visited Australia to teach counter-terrorism agencies how to defend against suicide attacks, stating that, 'police must prepare for all possible threats' for the approaching APEC summit. NSW Police Minister David Campbell confirmed that, 'we must always be prepared for the worst, which we hope will not occur' (O'Brien 2007, 6). It is argued that the same approach is required for the threat from maritime terrorism. This article has argued that the current protective regime, with an emphasis on the threat from small vessels, is inadequate. This inadequacy stems not only from a lack of appreciation of the consequences of an attack, but above all the failure of the government to promote an improved structural model for the policy making bureaucracy. Although it is impossible to provide total security in any situation, the current maritime security regime can be substantially improved. The highest levels of government and their policy makers need to make some difficult, expensive and potentially unpopular decisions as to the manner of improving the current maritime security regime.

Bibliography

- AAP. 2003. 'Protesters stop HMAS Sydney leaving harbour.' *Sydney Morning Herald*. 8 April. URL: <http://www.smh.com.au/articles/2003/04/08/1049567651003.html>. Consulted 20 April 2008.
- AAP. 2004. 'Terrorist attack on Australia inevitable, warns FBI expert.' *Sydney Morning Herald*. 16 March. URL: <http://www.smh.com.au/articles/2004/03/16/1079199194943.html?from=storyrhs>. Consulted 11 January 2006.
- ABS [Australian Bureau of Statistics]. 2006. 'International Trade in Goods and Services.' URL: [http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/ED66CE254E86E3D8CA257219001A7B89/\\$File/53680_sep%202006.pdf](http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/ED66CE254E86E3D8CA257219001A7B89/$File/53680_sep%202006.pdf). Consulted 12 January 2007.
- APSC [Australian Public Service Commission]. 2007. *Tackling Wicked Problems*. Canberra: AGPS.
- Abhyankar, J. 2002. 'Piracy and Maritime Violence: A continuing Threat to Maritime Industry.' ICC International Maritime Bureau. URL: <http://www.itopf.com/Abhyankar.pdf>. Consulted 15 January 2007.
- BBC News. 2008. 'US admits to Suez canal killing.' 26 March. URL: http://news.bbc.co.uk/2/hi/middle_east/7314225.stm. Consulted 10 April 2008.
- Barnes, R. 2008. 'Exxon Oil Spill Case May Get Closure.' *Washington Post*. URL: <http://www.washingtonpost.com/wp-dyn/content/story/2008/02/24/ST2008022400005.html>. Consulted 20 April 2008.
- Bateman, S., A. Bergin, M. Tsamenyi & D. Woolner. 2006. 'Integrated Maritime Enforcement and Compliance in Australia.' In *Towards Principled Oceans Governance - Australian and Canadian approaches and challenges*, eds. D. Rothwell & D. VanderZwaag. Abingdon: Routledge. (unpublished)
- Bouchard, J. 2005. 'New Strategies to protect America: Safer Ports for a More Secure Economy.' Center for American Progress. URL: http://www.americanprogress.org/kf/port_security.pdf. Consulted 20 January 2007.
- Campbell, T. & R. Burns. 2005. 'Terrorist Use of Commercial Shipping and Response: Leveraging Intelligence to Protect Ports and Seaways.' In *Combating Terrorism*, ed. R. Gunaratna. Marshall Cavendish International (Singapore) Private Limited.
- Carafano, J. 2007. 'Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea', Heritage Foundation. URL:

- http://www.heritage.org/Research/HomelandDefense/upload/bg_2041.pdf. Consulted 15 November 2007.
- Chalk, P. 2002. 'Threats to the Maritime Environment: Piracy and Terrorism.' RAND Stakeholder Consultation. Ispra. Italy. 28-30 October. URL: <http://www.rand.org/randeurope/about/news/seacur/piracyterrorism.chalk.pdf>. Consulted 14 October 2006.
- Commonwealth of Australia. 2004. *Transnational Terrorism: The Threat To Australia*, Canberra.
- [Australian Department of] Defence. 2003. 'Global Terrorism.' URL: <http://www.defence.gov.au/ans2003/section4.htm>. Consulted 11 January 2006.
- Discovery Channel. 'Shaped Charges.' URL: <http://www.youtube.com/watch?v=LudNqf56AFo&feature=related>. Consulted 10 April 2008.
- Dodd, M. 2007. 'Terror threat "the new totalitarianism".' *The Australian*. 22 May.
- Eisler, P., B. Morrison and T. Brook. 2007. 'Pentagon balked at pleas for safer vehicles.' *USA Today*. URL: http://www.usatoday.com/news/military/2007-07-15-ied-cover_N.htm. Consulted 15 April 2008.
- Gorman, E. 1992. 'Bomb Disposers Mark 21 Years in Ulster.' *The Times* (London). 7 November.
- Gunaratna, R. 1998. 'Trends in Maritime Terrorism – The Sri Lankan Case.' *Lanka Outlook*. vol. 4.
- Hoffman, B. 1998. *Inside Terrorism*. New York: Columbia University Press.
- MAST [Marine and Safety Tasmania]. 2007. 'New Security Requirements for Ships and Ports in Tasmania.' 5 July. URL: <http://www.mast.tas.gov.au/domino/mast/newweb.nsf/v-content/5069452A688A4133CA256ECC00206341>. Consulted 12 November 2007.
- O'Brien, N. 2007. 'APEC warning: prepare for anything.' *The Australian*, 22 May.
- Parliamentary Debates. House of Representatives. 2006. No 12. 7 September.
- Payne, L. 2007. 'Commentary' on M Buky. 'The Threat from Small Vessels.' *Maritime Studies*. 157:12.
- Raymond, C. 2006. 'Maritime Terrorism in Southeast Asia: A Risk Assessment.' *Terrorism and Political Violence* 18(2): 239 – 257.

- Richardson, D. 2004. 'ASIO Today.' 41 *AIAL Forum*.
- Richardson, M. 2004. *A Time Bomb for Global Trade*. Institute of Southeast Asian Studies. Singapore.
- Rittel, H. & M. Webber. 1973. 'Dilemmas in a General Planning Theory.' *Policy Sciences* 4: 155-169.
- Rodeman, C. 2003. 'In Search of an Operational Doctrine for Maritime Counterterrorism.' Naval War College. Newport.
- TRADOC [U.S. Army Training and Doctrine Command]. 2005. *A Military Guide to Terrorism in the Twenty-First Century*. Version 3, p. C-1. URL: <http://www.fas.org/irp/threat/terrorism/guide.pdf>. Consulted 15 October 2006.
- Todd, M. 2005. 'Chilling Warning: Terrorist Attack is Feasible.' *Sydney Morning Herald*. 14 October.
- Truss, W. 2005. 'Address To The Shipping Australia Limited Luncheon IMO World Maritime Day.' URL: http://www.ministers.dotars.gov.au/wtr/speeches/2005/WS12_2005.htm. Consulted 17 November 2007.
- Victorian Notices To Mariners. 2005. URL: <http://www.portofmelbourne.com/global/docs/13t-05pmc.pdf>. Consulted 10 April 2008.
- Yaukey, J. 2007. 'Troops make gains against IEDs.' *GlobalSecurity.Org*, 18 March. URL:<http://www.globalsecurity.org/org/news/2007/070318-ied-gains.htm>. Consulted 25 April 2008.

Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A – Almost Certain	H	H	E	E	E
B - Likely	M	H	H	E	E
C - Moderate	L	M	H	E	E
D - Unlikely	L	L	M	H	E
E - Rare	L	L	M	H	H

LEGEND
E: Extreme Risk
H: High Risk
M: Moderate Risk
L: Low Risk

Fig. 1. Qualitative risk analysis matrix

Source: Standards Australia. 1999. *Risk management AS/NZ 4360: 1999*, Standards Association of Australia, Strathfield. p. 35.