Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat

Lieutenant Commander Fiona McNaught, RAN

Introduction

The horrific effects of the 11 September 2001 terrorist attack on the World Trade Center and Pentagon in the United States shocked the world by graphically demonstrating the extraordinary lengths to which terrorist organisations will go in order to make political statements. Several recent terrorist attacks have also been made against maritime targets, including the USS *Cole* in 2000 and the tanker *Limberg* in 2002 (both in Yemen); passenger ferries in the Philippines and Indonesia; and oil installations in the Arabian Gulf. Evidence from intelligence sources suggests that terrorist groups such as Al'Qaeda routinely make use of commercial shipping to pursue their ends, and more disturbingly, have planned further attacks on maritime communications.[1]

The vulnerability of the maritime sector to exploitation by terrorist groups has driven the development of several maritime security measures designed to toughen the 'soft underbelly'[2] of the maritime transport sector. One key measure has been the 2004 entry into force of the International Ship and Port Facility Security (ISPS) Code, which imposes security related responsibilities on governments, shipping companies and port authorities, and provides guidelines for developing and implementing security plans for ports and ships. One year on from implementation, it is timely to ask whether the Code is shaping up as an effective maritime security measure in the fight against terrorism.

The aim of this paper is to assess whether the International Ship and Port Facility Security (ISPS) Code adequately addresses post-11 September 2001 maritime security threats.

As this Code is only one of a number of interrelated initiatives, an overview of the overall maritime security framework will be provided. This will set the context for an examination of the provisions of the ISPS Code and a review of its implementation to date. Strengths and weaknesses of the Code in addressing the maritime security threat will then be analysed, prior to an assessment being made of the adequacy of the ISPS Code to address the threat. In order to make such an assessment, however, it is first necessary to identify the nature and implications of the maritime security threat.

The maritime security threat

Maritime security encompasses a range of measures taken by maritime industry participants to address terrorism, sabotage, stowaways, illegal immigrants, asylum seekers, piracy and armed robbery at sea, seizure, pilferage, annoyance and surprise.[3] In this section the paper predominantly looks at the threat posed by terrorist activity, as this has been one of the main focuses of the maritime security arena since 11 September 2001. Terrorism is defined under the United Kingdom Prevention of Terrorism Act, 1976 as the 'use of violence for political ends [including] violence for the purpose of putting the public or any section of the public in fear'.[4]

In July 2003, the Maritime Transport Committee of the Organisation for Economic Co-operation and Development (OECD) conducted a vulnerability analysis of the risks to the

international maritime transport sector posed by terrorist organisations.[5] Four main areas of shipping were identified as presenting terrorist risk factors: cargo, vessels, people and money.

Two categories of cargo were identified as being vulnerable to terrorism—containerised cargo and bulk shipments. In 2001, individual container movements through ports numbered in the hundreds of millions, with approximately two per cent of those being subject to physical examination.[6] This low examination rate has contributed to the high level of international crime (such as drug smuggling) conducted using shipping containers, and represents an opportunity for terrorists. A point to note is that the threat exists along the entire supply chain, not just when the containers are in ships or ports. Potential terrorist uses for shipping containers include the concealment and delivery (detonation) of conventional, nuclear, chemical or biological weapons along the supply route (including vessels and port facilities), and the smuggling of people or weapons to aid the terrorist cause. Confirmation of this potential was provided by the October 2001 discovery within an Italian port of a well-equipped suspected terrorist inhabiting a modified container bound for North America.[7] With regards to bulk cargo shipments, much media attention is given to the destructive potential of Liquid Petroleum Gas (LPG) and Liquid Natural Gas (LNG) tankers.[8] In reality, it is unlikely that the explosion of an LPG or LNG tanker's cargo could be successfully rigged due to the relative modernity of these vessels and their robust security systems.[9] Bulk cargoes such as fertiliser-grade ammonium nitrate, which can be manipulated to cause significant explosions, pose a greater risk.[10]

Causing such an explosion would in effect make the vessel itself the weapon in a terrorist strike. Concerns have been raised about the suspected ownership by Al'Qaeda of a fleet of 15–18 bulk/general cargo vessels, which could conceivably be used to conduct 'suicide' operations against major population centres or economic targets in the same vein as the 9/11 aircraft strikes. To date, however, terrorists have generally used vessels as targets rather than weapons, attacking vessels to hijack cargo, hold crew members hostage or cause damage and injury.[11] Such activities have traditionally been conducted by 'pirates' operating in particular maritime zones such as the Indonesian archipelago and the Horn of Africa, however, there is increasing evidence to suggest an increasing nexus between piracy or armed attacks at sea and terrorist activity.[12] Other maritime terrorism could include using a vessel (of any size, depending on the intended effect) to launch an attack or to sink a vessel to disrupt infrastructure (for example, to block port access, effectively shutting down port operations).[13] The economic cost of disruption to operations of major trading ports[14] is likely to be unacceptably high, with potentially devastating effects on the world economy. To illustrate, it has been estimated that the cost of shutting down the operations of ports in the western US in October 2002 for 11 days (due to industrial action) was in excess of US$460 million.[15]

Personnel risk factors involve either risk *to* people (through attacks causing harm to passengers and/or crew), or risk *from* people within the maritime community. Evidence suggests that maritime crimes such as theft, smuggling, piracy and armed attacks at sea have been at times facilitated or aided by members of the sea-faring community.[16] Concerns are held about the abuse of the liberal rights of entry afforded to seafarers and the ease of obtaining falsified identity documents, resulting in illegal and undetected entry of criminals into foreign states.[17] The potential for terrorist organisations to exploit these weaknesses (for example, by inserting terrorist operatives without detection) is of major concern.

A final risk area for shipping is that of money. Terrorist organisations may operate vessels or fleets in order to generate funds and provide logistic support to their operations. The Liberation Tigers of Tamil Eelam (LTTE) have been doing so since the 1980s, and as previously mentioned, it

is believed that Al'Qaeda also own and control vessels. Proving such ownership is difficult due to opaque vessel and corporate registration requirements.[18]

Concerns over vulnerabilities such as those mentioned above have led to the recent adoption of several security initiatives, which can be viewed as part of an overarching maritime security framework.

The International Maritime Security Framework

The 1985 hijacking of the passenger vessel *Achille Lauro* off the coast of Egypt led to the 1992 adoption of international law in the form of the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention). Recent terrorist attacks on maritime vessels, including the previously mentioned attacks on the USS *Cole* and the tanker *Limberg,* demonstrated the SUA Convention's inadequacy to proactively address the maritime security threat posed by terrorism.[19] To this end, in December 2002, the International Maritime Organisation (IMO) convened a Diplomatic Conference addressing measures to strengthen maritime security and prevent and suppress acts of terrorism against shipping. This conference resulted in the adoption of a number of amendments to the SOLAS Convention**,** including, the addition of a new chapter detailing the new ISPS Code. Other SOLAS amendments included the requirement for ships to fit Automatic Identification Systems (AIS), to carry a Continuous Synopsis Record (CSR), and to standardise ship identification markings.[20]

The Conference also adopted resolutions addressing related maritime security issues that were thought to fall outside the scope of the SOLAS Convention and the ISPS Code.[21] Conference resolution 8—Enhancement of security in cooperation with the International Labour Organization (ILO)—invited the ILO to continue the development of a Seafarers' Identity Document, and provided for the establishment of a joint ILO/IMO Working Group on port security requirements.[22] Similarly, Conference resolution 9—Enhancement of security in cooperation with the World Customs Organization (WCO)—invited the WCO to consider measures to enhance security of containerised cargo and provided for IMO/WCO cooperation on this issue.[23] Resolution 5 provided for the promotion of technical cooperation and assistance for developing nations to improve maritime and port security infrastructure, including the provision of a Maritime Security Trust Fund. Finally, resolution 7 invited governments to consider establishing additional measures to enhance the security of ships and port facilities not covered by the ISPS Code.[24]

The background above sets the context for an examination of the ISPS Code provisions and analysis of its ability to address the maritime security threat posed by terrorism.

The ISPS Code

The ISPS Code comprises two parts, the first of which (Part A) contains detailed security requirements for governments, port authorities and shipping companies. Part B provides guidelines on how to meet these requirements, and is non-mandatory. The Code applies to passenger ships engaged on international voyages, cargo ships of 500 gross tonnage and upwards engaged on international voyages, mobile offshore drilling units and port facilities serving the afore-mentioned ships.

The rationale behind the development of the Code was that maritime security was essentially a risk management activity. As stated by a member of the Maritime Security Section of the IMO:

> The purpose of the ISPS Code is to provide a standardized, consistent framework for evaluating risk, enabling governments to offset changes in threat levels with changes in vulnerability for ships and port facilities.[25]

Part A of the Code specifies mandated risk mitigation measures and responsibilities relating to three security levels. Security level 1 represents the base level of appropriate[26] security measures to be maintained at all times. Security level 2 is where appropriate additional security measures are maintained for a period of time due to increased risk of a security incident. Under security level 3, further specific security measures are maintained for a limited period of time when a security incident is probable or imminent.[27]

Responsibilities of Contracting Governments under ISPS Part A include the responsibility to set appropriate security levels and provide guidance for protection from security incidents. They are also required to approve port facility assessments and port security plans, determine which ports are required to have a port facility security officer, and exercise control and compliance measures in accordance with SOLAS Regulations. Under security level 3, Contracting Governments are required to issue instructions and provide security information to affected ships and ports. They are also responsible for conducting security verifications of, and issuing International Ship Security Certificates (ISSC) to, ships flying their flag, although the Contracting Government may delegate this responsibility to a recognised security organisation.[28]

Shipping companies are required under Part A to appoint a Company Security Officer (CSO) for the company and a Ship Security Officer (SSO) for each of its ships. Responsibilities of these positions are detailed within the Code, including the requirement to conduct training and drills. Specifically, the CSO is responsible for ensuring that each ship has conducted a Ship Security Assessment (SSA) and developed and implemented a Ship Security Plan (SSP). The SSP indicates the minimum security measures the ship is to enforce at security level 1,[29] additional security measures required for security level 2, and possible preparatory actions for security level 3.[30] Similar requirements are placed upon Port Facility Operators. Port Facility Security Officers are responsible for ensuring Port Facility Security Assessments (PFSA) are conducted and Port Facility Security Plans (PFSP) are developed and implemented.[31] A point to note is that the ISPS provisions relating to port facilities relate only to the ship/port interface.[32]

Part B of the ISPS Code[33] provides specific guidance on how to carry out the responsibilities mandated by Part A. This includes guidance on areas of potential vulnerability and control methods to address these in security plans. The focus of Part B guidance is on protective measures *for* ships alongside at port facilities. Threats posed *by* ships to port facilities are not specifically addressed, however, those conducting PFSPs are advised to consider adapting the guidance to address such threats.[34]

Implementation of the Code

The ISPS Code was promulgated in 2003, and came into force 1 July 2004. In maritime industry terms, this was a brief timeframe in which to complete the Code's numerous requirements. While there were concerns held in some quarters on the 'unrealistic'[35] timeframe and potential disruptions to international trade, the predicted chaos did not eventuate.[36] On the day the Code came into force, more than 86 per cent of ships and 69 per cent of port facilities subject to the Code had their security plans approved.[37] By February 2005, the IMO reported that ships had reached a 'high degree of compliance' with minimal disruption to world trade, and that Contracting Governments had approved security plans for 97 per cent of declared port facilities.[38]

Teething problems were anticipated in the initial implementation of the Code, and the IMO attempted to mitigate these through the conduct of the technical assistance program and numerous regional seminars.[39] Nevertheless, implementation problems included a bottleneck in the issue

of ISSCs (with only 56 per cent of certificates being issued by 1 July 2004[40]), and problems implementing the Code in some regions (for example Africa and some countries in Eastern Europe).[41] The United States has been most visibly active in implementing and enforcing the ISPS,[42] with 8.5 per cent of inspections in the first month resulting in enforcement actions including denial of entry, expulsion or detention. Most non-compliant vessels were reported as belonging to Flags of Convenience registers. Interestingly, a significant proportion was also smaller than 500 tons.[43] The US Coast Guard also named seven countries as being non-compliant with the port facility requirements of the ISPS Code.[44]

Australia is signatory to the SOLAS Convention and therefore is subject to the ISPS Code. The *Maritime Transport and Offshore Facilities Security Act 2003* implements the security requirements of SOLAS and the ISPS Code in Australia, and allows for the establishment of the Maritime Security Identification Card.

EFFECTIVENESS OF THE ISPS CODE

Having considered the content and implementation of the ISPS Code, an analysis of the Code's strengths and weaknesses should provide the basis from which to assess the Code's effectiveness in addressing the maritime threat posed by terrorism.

ISPS code weaknesses

One major weakness of the Code is the inability of the IMO to enforce its Regulations—it can only monitor compliance.[45] Enforcement is the domain of Contracting Governments, most often as a part of Port State Control regimes. As previously mentioned, the USCG has been particularly active in this regard since the implementation of the ISPS Code.

As previously stated, the ISPS Code is based on the principles of risk management. One aspect of ISPS implementation that attracts a great deal of criticism relates to the differing risk profiles and standards applied between nations. There are several dimensions to this problem. Firstly, as each Contracting Government is responsible for determining and enforcing appropriate security measures for its ships and ports, there are bound to be significant differences between nations in the standards of those measures. This is mitigated to some extent by initiatives such as the IMO Integrated Technical Co-operation Program and the US Coast Guard's International Port Security (IPS) Program.[46] Secondly, some Contracting Governments, particularly Flag of Convenience registries, have been identified as either corrupt (and therefore vulnerable to exploitation by terrorist groups),[47] or as lacking the resources or expertise to enforce acceptable standards.[48] While governments may contract out some of their security responsibilities to RSOs (often Classification Societies) the expertise of these organisations in the maritime security field varies significantly.[49]

Applicability of the ISPS Code to vessel types is also a weakness when it comes to addressing the terrorist threat. The ISPS Code does not apply to many vessels that are either vulnerable to, or capable of, terrorist attack or exploitation. These include fishing vessels, high speed container vessels built prior to July 2001, vessels not engaged in international voyages (including inter-island ferries similar to the ones attacked in recent years in Southeast Asian waters), and cargo ships less than 500 ton. Part B of the ISPS Code advises Contracting Governments to establish security measures for vessels not covered by Part A of the Code, however, this is not mandatory, and is therefore unlikely to be heeded by some nations (particularly Flag of Convenience registries).

As mentioned earlier, port security measures covered by the ISPS Code are limited to matters involving the ship/port interface. More comprehensive port security measures are subject to further development by such bodies as the ILO/IMO Working Group. This includes the ongoing work on Seafarers Identity Documents, which is not likely to be resolved in the immediate future due to differing opinions on the level of information to be provided in these documents.[50] In the interim, the onus is on Port States to implement appropriate port security measures to mitigate the risk of terrorist operatives gaining access to ports or vessels.

Similarly, the ISPS Code's narrow focus on security measures to be taken in ships and ports ignores the major issue of container security, and the vulnerability of the supply chain to tampering by criminals (including terrorists). While the WCO is working on this issue (with ILO input in accordance as previously mentioned), achieving an industry standard internationally is thought by some to be almost unachievable[51] and perhaps disproportionately expensive, raising the costs of international trade.[52] The United States has developed unilateral initiatives to address cargo security, including the Container Security Initiative (CSI) and the Customs–Trade Partnership Against Terrorism (C–TPAT). These initiatives target security measures along the entire supply chain, thereby expanding the more narrow focus of the ISPS. These initiatives may very well provide a model for the WCO in developing internationally binding cargo security measures.

The ISPS Code is preventative in nature and therefore does not address the issue of response to attacks or remediation issues following an attack.[53] Contracting Governments are expected to address this issue according to national legislation. In Australia's case, responses to maritime security incidents will be addressed through domestic measures such as the National Counter-Terrorism Plan.

ISPS Code strengths

One benefit of the ISPS Code over the SUA Convention is the more streamlined approval process involved in making amendments to the Code (due to the 'tacit acceptance' provision of the SOLAS Convention. This will enable a quicker response to evolving nature of the terrorist threat.

Despite some concerns about the costs of implementing maritime security measures (not only for ISPS, but also for related initiatives such as the CSI), there have been positive flow-on effects as a result of stricter controls on container tracking and manifesting and the consequent cost savings from reduced theft and pilferage.[54]

The adoption of the ISPS Code and related initiatives may yet address some of the issues surrounding Flag of Convenience registries. Dissatisfaction with the performance of flag state administration under the new regime may influence shipping nations to re-flag with more efficient and reputable registries. Alternatively, those flag states may improve their performance in order to compete for ship registration.

Perhaps the greatest strength of the ISPS Code is the provision of a common baseline for international cooperation on the issue of maritime security. Implementation has gone relatively smoothly to date, indicating a strong drive to proactively and collectively address maritime security. The level of awareness of maritime vulnerability to terrorist attack has been increased through the implementation of Part A of the ISPS Code, and if nothing else, the maritime industry should be better prepared for any future terrorist attacks.

Overall assessment

Taking into account these strengths and weaknesses, an assessment can be made on the ability of the ISPS Code to address the maritime security risk areas of cargo, vessels, people and money.

The implementation of the ISPS Code is unlikely to adequately mitigate the risk posed by containerised cargo, as it is focused on the narrow area of ship security and the ship/port interface. The terrorist threat (for example the placement of a weapon of mass destruction within a shipping container) is more likely to be introduced during another phase of the supply chain. This said, complementary initiatives within the broader maritime security framework (such as CSI and C–TPAT) are addressing this shortfall.

While implementation of Part A of the Code has probably reduced the vulnerability of individual ships to attack while in port (through more robust security practices), the Code provides scant protection against acts of terrorism designed to use vessels as weapons themselves. Many vessels that may be utilised in such a way by terrorists are not subject to the provisions of the Code.

The threat to maritime security posed by personnel (for example use of seafarer status to insert terrorist operatives) is not addressed by the ISPS Code, although the ILO/IMO Working Group progressing work on this area is the result of a complementary initiative.

Terrorist organisations controlling their own vessels or fleets in order to finance their operations are unlikely to be impacted by the implementation of the ISPS Code, as these ships are often run as legitimate business concerns and true ownership of ships is still difficult to assess.

Conclusion

The above assessment highlights the extremely limited scope of the ISPS Code to address the main risk factors to maritime security in light of the terrorist threat. This said, the ISPS is only one of an interrelated set of maritime and other broader security measures designed to reduce the transport chain's vulnerability to security incidents, and specifically, terrorist attack. The ISPS must therefore be viewed not as a stand-alone solution to the maritime security threat, but rather as one component of a system in the fight against terrorism. What is clear is that other key components of this system need to be addressed in order to fill the gaps that currently exist. This is particularly the case with regard to the security of containerised cargo and the issue of Seafarers Identity Documentation.

Where the ISPS Code has been successful is in the raising of the awareness level of the maritime community on issues of maritime security. This is a step in the right direction, noting that the goal of the IMO is 'to create the necessary security culture and raise our defences so high that the shipping industry does not become a target for terrorist activities'.[55] With the security culture in place and strengthening, it is now time to focus on the raising of those defences.

Endnotes

1. Joshua Ho, 'The Security of Sea Lanes in Southeast Asia', *Military Technology*, May 2005, Vol. 29, Iss. 5, Bonn.
2. Hartmut Hesse & Nicolaos L. Charalambous, 'New Security Measures for the International Shipping Community', *WMU Journal of Maritime Affairs*, 2004, Vol. 3, No. 2, p. 131.
3. Peter Heathcote, 'An Explanation of the New Measures for Maritime Security Aboard Ships and in Port Facilities', *Maritime Studies*, No. 137, July/August 2004, p. 14.
4. ibid.
5. Organisation for Economic Co–Operation and Development (OECD) Maritime Transport Committee, *Security in Maritime Transport: Risk Factors and Economic Impact*, OECD, Paris, July 2003.
6. OECD, p. 8.
7. OECD, p. 9.
8. Joshua Ho, 'The Security of Sea Lanes in Southeast Asia'. For example, the April 2005 Current Awareness Bulletin on the International Maritime Organisation website <http://www.imo.org/InfoResource.html> lists two articles specifically addressing the potential of gas bulk carriers as terrorist targets.
9. As cited in OECD, p. 12, a direct Exocet missile hit on a LNG cargo tank during the Iran–Iraq war did not cause an explosion.
10. OECD, p. 12.
11. OECD, p. 13.
12. John F. Bradford, 'The Growing Prospects for Maritime Security Cooperation in Southeast Asia', *Naval War College Review*, Summer 2005, Vol. 58, Iss. 3, Washington.
13. OECD, p. 13.
14. Major trading ports include such ports as Long Beach/Los Angeles, Hong Kong, Singapore, Rotterdam and Antwerp.
15. Commonwealth of Australia, *Costs of Terrorism and the Benefits of Working Together*, Department of Foreign Affairs and Trade, Economic Analytical Unit, Canberra, October 2003, p. 14.
16. OECD, p. 15.
17. OECD, p. 15.
18. OECD, pp. 16–17.
19. Tamara Renee Shie, 'Ports in a Storm? The Nexus Between Counterterrorism, Counterproliferation, and Maritime Security in Southeast Asia', *Issues & Insights*, Vol. 4, No. 4, Pacific Forum CSIS, Honolulu, July 2004, p. 8. It is a reactive Convention, providing for punitive action to be taken against persons committing unlawful acts against ships. The IMO is due to convene a Diplomatic Conference in October 2005 to discuss proposed amendments to the SUA Convention including a substantial broadening of the range of offences under the Convention and the introduction of provisions for boarding vessels suspected of being involved in terrorist activities (Source: IMO website <http://www.imo.org>).
20. International Maritime Organization, *International Ship and Port Facility Security Code and SOLAS Amendments adopted on 12 December 2002*, 2003 Edition, London, pp. 108–112.
21. The SOLAS Convention's main focus is on the safety of ships and seafarers at sea, and therefore its scope to address wider port issues (other than ship/port interface matters) and supply chain security is limited.
22. This Working Group has developed and implemented a Code of Practice for the security of all port areas (adopted May 2004).
23. To this end, a Memorandum of Understanding between the IMO and WCO was signed in July 2001.
24. International Maritime Organization, *ISPS Code and SOLAS Amendments*, pp. 128–138.

25. Chris Trelawny, 'Maritime Security: Implementation of the ISPS Code', 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference, Dar es Salaam, 3–4 February 2005, p. 4.
26. 'Appropriate' in this context is not defined in Part A of the ISPS Code, as each ship and port facility is expected to undertake specific risk assessment in order to determine the level of protective security measures required. There is some limited direction provided for security level 1 in Section 7.2 of the Code (Part A), with further guidance provided in Part B.
27. International Maritime Organization, *ISPS Code*, p. 8.
28. ibid., pp. 9–10, 24–25.
29. This includes such activities as controlling access to the ship; monitoring restricted areas, deck areas and areas adjacent to the ship; supervising the handling of cargo and stores; and ensuring the availability of security communications.
30. International Maritime Organization, *ISPS Code*, pp. 11–18.
31. International Maritime Organization, *ISPS Code*, pp. 18–23.
32. Peter Heathcote, 'An Explanation of the New Measures for Maritime Security Aboard Ships and in Port Facilities', p. 15.
33. International Maritime Organization, *ISPS Code*, pp. 37–104.
34. International Maritime Organization, *ISPS Code*, p. 37.
35. Robert Botelho, 'Maritime Security: Implications and Solutions', *Sea Technology*, March 2004, Vol. 45, No. 3, p. 16.
36. Robert Wright, 'World Ports', *Financial Times*, London, 23 May 2005, p. 1.
37. International Maritime Organization, Press briefing, 'Secretary General Mitropoulous pays tribute to the efforts made to implement the ISPS Code', 1 July 2004, <http://www.imo.org/newsroom>.
38. International Maritime Organization, Press briefing, 'Maritime Security on agenda as USCG Commandant visits IMO', 17 February 2005, <http://www.imo.org/newsroom>.
39. These seminars were provided under the IMO Global Programme on Maritime and Port Security.
40. The backlog of ISSCs has since been cleared, and the compliance rate is now nearing 100 per cent.
41. International Maritime Organization, Press briefing, 'Security compliance shows continued improvement', 6 August 2004, <http://www.imo.org/newsroom>.
42. The US have indicated that ISPS Part B will become mandatory, as have the UK (Source: Robert Botelho, 'Maritime Security: Implications and Solutions', p. 16).
43. 'Team Effort with Maritime Industry Helps USCG Tackle New Security Rules', *Seafarers Log*, August 2004, accessed on–line at <http://proquest.com>.
44. Shashi Kumar, 'U.S. Merchant Marine and Maritime Industry Review', *United States Naval Institute Proceedings*, May 2005, Vol. 131, Iss. 5, Annapolis, p. 105.
45. Catherine Zara Raymond, 'The Challenge of Improving Maritime Security', *Journal of the Australian Naval Institute*, Summer 2005, No. 115, Fyshwick, p. 15.
46. This program involves assessment by the USCG of the effectiveness of anti–terrorism measures in place at foreign ports that are visited by vessels that also visit the US.
47. Robert Botelho, 'Maritime Security: Implications and Solutions', p. 16.
48. Catherine Zara Raymond, 'Australia's New Maritime Security Strategy', *Journal of the Australian Naval Institute*, Summer 2005, No. 115, Fyshwick, p. 14.
49. Peter Heathcote, 'An Explanation of the New Measures for Maritime Security Aboard Ships and in Port Facilities', p. 17.
50. Shashi Kumar, 'U.S. Merchant Marine and Maritime Industry Review', p. 110. Even the US, which is progressing unilateral action to introduce a biometric identification card, does not expect to establish standards for the card until

late 2006 (Source: Edmonson, R.G., 'Transport ID Card Awaits Rules', *Journal of Commerce Online Edition*, 29 June 2005, New York, <http://proquest.umi.com>).

51. Nick Brown & Richard Scott, 'ISPS Code steps up security for ports and shipping', *Jane's Navy International*, September 2004, p. 23.

52. The Australian Customs Service estimated that installation of equipment to meet CSI inspection requirements would only increase current inspection rates by 5 per cent (Source: Shie, Tamara Renee, 'Ports in a Storm?', p. 28).

53. International Maritime Organization, *ISPS Code*, p. 4. The revised SUA Convention is, however, expected to provide the legal basis for the arrest, detention and extradition of terrorists in the event of a terrorist attack against shipping (Source: International Maritime Organization, Press briefing, 'Draft SUA protocols ready for October Conference', 3 May 2005, <http://www.imo.org/newsroom>).

54. 'Cargo Security Cuts Crime', *Traffic World*, 5 May 2005, Newark, p. 1.

55. International Maritime Organization, Press briefing, 'Continued improvement in ISPS Code implementation', 30 June 2004, <http://www.imo.org/newsroom>.

Bibliography

Australian Strategic Policy Institute (ASPI), 'Future unknown: The terrorist threat to Australian maritime security', Canberra, dated 19 April 2005. Accessed on-line at <http://www.aspi.org.au>.

Botelho, Robert, 'Maritime Security: Implications and Solutions', *Sea Technology*, March 2004, Vol. 45, No. 3.

Bradford, John F., 'The Growing Prospects for Maritime Security Cooperation in Southeast Asia', *Naval War College Review*, Summer 2005, Vol. 58, Iss. 3, Washington.

Brew, Nigel, 'Ripples from 9/11: the US Container Security Initiative and its Implications for Australia', Commonwealth of Australia Parliamentary Current Issues Brief No. 27 2002-03, Canberra, 13 May 2003.

Brown, Nick & Scott, Richard, 'ISPS Code steps up security for ports and shipping', *Jane's Navy International*, September 2004.

'Cargo Security Cuts Crime', *Traffic World*, 5 May 2005, Newark.

Commonwealth of Australia, *Costs of Terrorism and the Benefits of Working Together*, Department of Foreign Affairs and Trade, Economic Analytical Unit, Canberra, October 2003.

Commonwealth of Australia, Department of Transport and Regional Services Maritime Security website, <http://www.dotars.gov.au/transsec>.

Commonwealth of Australia, *Maritime Transport and Offshore Facilities Security Act 2003*, accessed on-line at <http://www.comlaw.gov.au/ComLaw/Legislation>.

Edmonson, R.G., 'Ports and Security', *Journal of Commerce*, 18 April 2005, New York, p. 1.

Edmonson, R.G., 'Transport ID Card Awaits Rules', *Journal of Commerce Online Edition*, 29 June 2005, New York, <http://proquest.umi.com>.

Griffett, Trevor, 'The Impact of ISPS Compliance on Shipowners: Security Awareness – the new safety outcome', *Port & maritime security & counter-terrorism summit*, Melbourne, 28 April 2005.

Heathcote, Peter, 'An Explanation of the New Measures for Maritime Security Aboard Ships and in Port Facilities', *Maritime Studies*, No. 137, July/August 2004.

Hesse, Hartmut & Charalambous, Nicolaos L., 'New Security Measures for the International Shipping Community', *WMU Journal of Maritime Affairs*, 2004, Vol. 3, No. 2.

Ho, Joshua, 'The Security of Sea Lanes in Southeast Asia', *Military Technology*, May 2005, Vol. 29, Iss. 5, Bonn.

International Maritime Organization, website, <http://www.imo.org>.

International Maritime Organization, 'FAQ on ISPS Code and maritime security', accessed on-line at <http://www.imo.org/newsroom>, 23 August 2005.

International Maritime Organization, *International Ship and Port Facility Security Code and SOLAS Amendments adopted on 12 December 2002*, 2003 Edition, London.

International Maritime Organization, MSC Circular 1112, 'Shore Leave and Access to Ships under the ISPS Code', London, 7 June 2004.

International Maritime Organization, MSC Circular 1132, 'Guidance Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code', London, 14 December 2004.

International Maritime Organization, Press briefing, 'Draft SUA protocols ready for October Conference', 3 May 2005, <http://www.imo.org/newsroom>.

International Maritime Organization, Press briefing, 'Secretary General Mitropoulous pays tribute to the efforts made to implement the ISPS Code', 1 July 2004, <http://www.imo.org/newsroom>.

International Maritime Organization, Press briefing, 'Security compliance shows continued improvement', 6 August 2004, <http://www.imo.org/newsroom>.

International Maritime Organization, Press briefing, 'Continued improvement in ISPS Code implementation', 30 June 2004, <http://www.imo.org/newsroom>.

International Maritime Organization, Press briefing, 'Maritime Security on agenda as USCG Commandant visits IMO', 17 February 2005, <http://www.imo.org/newsroom>.

Keane, Angela Greiling, 'Megaports a Megaflop?', *Traffic World*, 16 May 2005, Newark.

Kumar, Shashi, 'U.S. Merchant Marine and Maritime Industry Review', *United States Naval Institute Proceedings*, May 2005, Vol. 131, Iss. 5, Annapolis.

Organisation for Economic Co-Operation and Development (OECD) Maritime Transport Committee, *Security in Maritime Transport: Risk Factors and Economic Impact*, Paris, July 2003.

Piercey, Michele, 'Piracy and the risks of maritime terrorism: How significant are these threats?', *Geddes Papers 2004*, Australian Defence College, Canberra, 2004.

Raymond, Catherine Zara, 'Australia's New Maritime Security Strategy' and 'The Challenge of Improving Maritime Security', *Journal of the Australian Naval Institute*, Summer 2005, No. 115, Fyshwick.

Shie, Tamara Renee, 'Ports in a Storm? The Nexus Between Counterterrorism, Counterproliferation, and Maritime Security in Southeast Asia', *Issues & Insights*, Vol. 4, No. 4, Pacific Forum CSIS, Honolulu, July 2004.

'"Team Effort" with Maritime Industry Helps USCG Tackle New Security Rules', *Seafarers Log*, August 2004, accessed on-line at <http://proquest.com>.

Trelawny, Chris, 'Maritime Security: Implementation of the ISPS Code', 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference, Dar es Salaam, 3–4 February 2005, accessed on-line at <http://www.imo.org>.

Unisys Australia, 'Insiders uncomfortable with the state of Supply Chain Security', Sydney, 28 April 2005, accessed on-line at <http://www.unisys.com.au>.

US Department of Homeland Security, *Container Security Initiative Fact Sheet,* US Customs and Border Protection, Washington, April 2005.

US Department of Homeland Security, 'International Port Security (IPS) Program', United States Coast Guard Navigation and Vessel Inspection Circular No. 02–05, Washington, 15 February 2005.

Wright, Robert, 'World Ports', *Financial Times*, London, 23 May 2005.

Wright, Robert, 'Worldwide Security', *Financial Times*, London, 9 May 2005.