IDSS COMMENTARIES (62/2004)

IDSS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of IDSS.

The Challenge of Improving Maritime Security

An assessment of the implementation of the ISPS Code and initial responses as to its effectiveness

Catherine Zara Raymond*

9 December 2004

Immediately following the shocking September 11th World Trade Centre attacks in New York, governments around the world hurried to assess their vulnerability to highly organised terrorist groups willing to sacrifice many lives to achieve their aims. Although the initial focus was on the vulnerability of the air transport system, attention soon turned to the maritime sector - that is, the vulnerability of port infrastructure and commercial shipping to a maritime terrorist attack.

Following requests by the US, the International Maritime Organization (IMO) - a specialized maritime agency of the United Nations - developed an international maritime security code that would address some of the perceived vulnerabilities found to be present in most states' maritime security systems. In December 2002, adoption of the new code – the International Ship and Port Facility Security Code (ISPS Code) – was made mandatory under international law.

The Code, which entered into force on 1st July 2004, covers: Cargo vessels over 500 gross tonnes on international voyages, port facilities serving ships on international voyages, passenger ships and mobile offshore drilling units.

It requires ships and port facilities to carry out security assessments, after which ships are required to create ship security plans, appoint ship security officers and company security officers. Ships are also required to carry certain onboard equipment. Port facility requirements include the creation of port facility security plans and port facility security officers. Port facilities are also obliged to keep certain security equipment.

As each ship and port facility represent different levels of risk or are under varying levels of threat, the ISPS Code requires the contracting governments to set an appropriate security level, in order to communicate this to the relevant parties. The security levels are 1, 2, and 3, which correspond to normal, medium, and high threat situations, respectively. When there is a heightened risk of a security incident, the security level is raised. Ships and terminals are then required to take extra protective security measures.

Has the ISPS Code been successfully implemented?

Despite some initial hiccups, implementation of the Code has largely been a success. According to the latest figures, 89.5 per cent of over 9000 declared port facilities now have their port facility plans approved and 90 per cent of ships required to comply with the ISPS Code have now had there International Ship Security Certificates issued.

Singapore was one of the success stories. Through close cooperation with the port operators and ship owners, its port facilities and ships met the ISPS Code requirements by the 1st July 2004 deadline. In fact Singapore' s container ships began to be certified as ISPS compliantten months before the deadline.

On the other hand, implementation of the Code in Africa has been less successful. Only half of the countries in Africa to which the Code applies have had their port facility plans approved. Former Soviet and Eastern European countries are also lagging far behind in their implementation.

Has the ISPS Code reduced maritime vulnerability?

In theory, compliance with the Code should reduce the vulnerability of port facilities and ships to maritime attacks by terrorists and pirates. Reducing the vulnerability of ships to attack from pirates is particularly important in Southeast Asia, which is home to one of the world's busiest and economically valuable shipping lanes - the Straits of Malacca, and also the world's most pirate plagued nation - Indonesia. Pirate attacks in Indonesian waters, or armed robbery as it is often referred to, account for a quarter of the global total. It has been estimated that across the globe, pirate attacks result in losses of USD25 billion each year.

However, according to evidence gathered by the International Maritime Bureau (IMB), from its Piracy Reporting Centre in Kuala Lumpur, while there has been a decrease in the number of pirate attacks reported worldwide in the first nine months of 2004, it is still expected that attacks will spike towards the end of the year, due to the delay in the reporting of attacks by some countries. Also, the number of casualties from pirate attacks has remained high. Thirty crewmembers have been killed so far in 2004, as opposed to only twenty at this point last year.

Are there flaws in the new security code?

A number of problems have started to come to light, which point to serious deficiencies in the Code itself and in its implementation.

One of the main problems is that the IMO is powerless when it comes to enforcing its regulations. It can only monitor compliance. When we combine the IMO's inability to enforce its regulations with the simple fact that in may of the world's poorer nations there is a lack of resources and people with sufficient expertise to enforce the standards that are

acceptable to the shipping community at large, the result is only a veneer of compliance with the new security standards. In order to address this problem the IMO has developed a new 'train-the-trainer' programme which is intended to aid ISPS Code implementation. Under the programme qualified and approved instructors will train those responsible for training and implementing the ISPS Code in the various countries.

In another initiative designed to address this issue, the US Coast Guard (USCG) is beginning a series of ISPS Code checks. They intend to visit 135 countries over the next three years, in order to verify the various countries' compliance with the ISPS Code. Despite the declared aim of these inspections, namely the "sharing" and "alignment" of security practices, the USCG has warned that enforcement actions will be taken against ships arriving from errant harbours. Such measures could range from controlling a ship's movement in harbour, armed escort, cargo delays or complete denial of entry to a US port. The US has also warned that it will take punitive measures against countries that do not allow the inspections to take place.

Meeting the ISPS Code requirements places substantial additional costs on ship owners. Firstly, ship owners have in some cases had to increase their crew size. Secondly, costs incurred by ports that have also had to introduce new security measures under the Code are being passed onto the ship owners in the form of extra charges for using the particular port. The most recent example is the Port of Brisbane' which will charge its port users an extra AUD1.4 million next year, in order to cover charges it incurred mainly as a consequence of the implementation of the ISPS Code. This will have repercussions throughout the global economy, possibly leading to price increases on imported and exported goods. While security is recognised as being one of the costs of doing business in the post 9/11 world, the ISPS Code has yet to prove itself a worthwhile weapon in the arsenal of maritime security.

A glaring flaw in the ISPS Code is that it only applies to ships over 500 gross tonnes that are employed on international voyages. Therefore, it does not apply to most fishing vessels and tugboats, which are usually under 500 gross tonnes. It also does not apply to the many merchant ships engaged in domestic trade. As a result, there will be a substantial number of ships operating in Southeast Asian waterways that are not covered by the Code. This is a worrying situation given the recent spate of attacks on tugboats in the Malacca Straits. In the latest attack which took place on 30 November, the captain and chief engineer of a Malaysian tugboat were kidnapped.

In an effort to address this problem, Singapore's port authority has introduced additional measures such as the Harbour Craft Security Code to ensure that harbour craft plying its port waters comply with general security standards. Also, small vessels that are not required to comply with the ISPS Code are also required to fill up a 'Ship Self-Security Assessment Checklist' prior to entering the port waters.

The ISPS Code clearly has a number of limitations and it will therefore not significantly reduce the vulnerability of the maritime sector to attack from terrorists or pirates. However, as Captain Mukundan, of the IMB states: "The ISPS code is a necessary first step in establishing a global maritime security framework." In other words it forms a baseline standard which can be built upon in the future. Alone, it cannot defeat the challenges facing maritime security.

* Catherine Zara Raymond is an Associate Research Fellow in the Maritime Security Programme at the Institute of Defence and Strategic Studies, Nanyang Technological University.