No. 154

The use of SOLAS Ship Security Alert Systems

Thomas Timlen

S. Rajaratnam School of International Studies

Singapore

5 March 2008

With Compliments

The S. Rajaratnam School of International Studies (RSIS) was established in January 2007 as an autonomous School within the Nanyang Technological University. RSIS's mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education in international affairs with a strong practical and area emphasis

- Conduct policy-relevant research in national security, defence and strategic studies, diplomacy and international relations

- Collaborate with like-minded schools of international affairs to form a global network of excellence

Graduate Training in International Affairs

RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (MSc) degrees in Strategic Studies, International Relations, International Political Economy, and Asian Studies as well as an MBA in International Studies taught jointly with the Nanyang Business School. The graduate teaching is distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Over 150 students, the majority from abroad, are enrolled with the School. A small and select Ph.D. programme caters to advanced students whose interests match those of specific faculty members.

Research

RSIS research is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS, founded 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2002), the Centre of Excellence for National Security (CENS, 2006), the Centre for the Advanced Study of Regionalism and Multilateralism (CASRM, 2007); and the Consortium of Non-Traditional Security Studies in ASIA (NTS-Asia, 2007). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The S. Rajaratnam Professorship in Strategic Studies brings distinguished scholars and practitioners to participate in the work of the Institute. Previous holders of the Chair include Professors Stephen Walt, Jack Snyder, Wang Jisi, Alastair Iain Johnston, John Mearsheimer, Raja Mohan, and Rosemary Foot.

International Collaboration

Collaboration with other professional Schools of international affairs to form a global network of excellence is a RSIS priority. RSIS will initiate links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABSTRACT

The requirement for all merchant ships plying international trading routes to be equipped with Ship Security Alert Systems stemmed from the many initiatives to protect the world from terrorist threats that were developed in the aftermath of the 911 attacks in the United States in 2001.

As governments moved forward to develop global requirements at the International Maritime Organization, seafarers remained skeptical as to whether the measures would serve to protect them or, to the contrary, endanger their safety. Such skepticism appears to have subsequently abated as seafarers have begun to use the Ship Security Alert Systems when under attack by pirates and armed robbers.

The responses of shore-side entities to the alerts are varied. Today, the flag states responsible for the safe operation of the ships within their registries may establish their own response plans and arrangements. For many, cooperation with other nations is not only advantageous but crucial as few Flag States have the necessary resources to protect the ships flying their flags in all parts of the world.

There are, however, many opportunities that exist to link national, regional and even commercial arrangements designed to protect merchant shipping, which in turn could lead to the establishment of an international mechanism for coordinating timely and effective responses to ship security alerts. Furthermore, solutions may be found in enabling ship security alert systems to contact the responders directly, as this has been done effectively with regard to piracy attacks.

****

Thomas Timlen was previously Head of the Baltic and International Maritime Council's Security and International Affairs Department. Whilst with BIMCO he was engaged with the work at the International Maritime Organization that developed the SOLAS International Ship and Port Facility Security Code and other amendments to the convention that included the Ship Security Alert System requirement.

The use of SOLAS Ship Security Alert Systems

Exploring how Flag States manage ship security alerts, and the potential to improve the effectiveness of rapid response management to prevent acts of terrorism.

INTRODUCTION

The Safety of Life at Sea (SOLAS) Convention requires that nearly all merchant ships are now equipped with ship security alert systems. These systems were developed at the International Maritime Organization together with several other requirements, all with one common goal; to reduce the risks of ships being used or being targeted by terrorists[1].

Ship security alert systems are designed as silent alarms which, when activated, do not issue the initial alert to nearby security forces. The alert in most cases is first received by the ship's owner, then passed to the ship's flag state, and finally to the national authorities of the coastal states in the immediate vicinity of the ship.

Today, nearly four years after it became mandatory for merchant ships to be equipped with ship security alert systems, this paper attempts to review how the systems have been used in practice, the benefits and shortcomings of the systems, and potential opportunities that may exist to enhance their effectiveness.

Although there have been no cases identified involving acts of terrorism in which ship security alert systems were used, one can make observations and draw conclusions from the few acts of terrorism that have involved merchant ships prior to the requirement, as well as from incidents of piracy, some of which have involved the use of ship security alert systems.

Finally, in consideration of a high frequency of false alerts sent from ships, and the cumbersome alert routing process, one may wonder if the security alert systems as they are now designed could prevent an act of terrorism. This paper raises several serious concerns on this point, and offers several recommendations aimed at enhancing the potential for these systems to succeed.

Origins of the Ship Security Alert System

At 7:59 AM on 11 September 2001, American Airlines Flight 11 took off from Boston's Logan Airport. 47 minutes later, and only 27 minutes after a flight attendant on board informed colleagues on the ground that a hijacking was underway, Flight 11 crashed into the North Tower of the World Trade Center in New York.[2] Three other hijacked planes also took all on board and many more on the ground to fiery and

[1] On 20 November 2001 the International Maritime Organization (IMO) Assembly adopted Resolution A.924(22) which amongst other things requested the IMO Secretary-General "to take appropriate measures within the Integrated Technical Co-operation Programme to assist Governments to assess, put in place or enhance, as the case may be, appropriate infrastructure and measures to strengthen port safety and security so as to prevent and suppress terrorist acts." This resolution led to the development of the security-related amendments to the SOLAS Convention including the ship security alert system requirements.

[2] The times shown appear in many sources that document the events of 11 September 2007.

violent deaths before anything could effectively be done to mitigate the loss of life and devastation.

After the terrorist attacks against the United States on 11 September 2001 many initiatives were launched aimed at the prevention of acts of terrorism.

With respect to merchant shipping, the organizations that explored the potential need to develop new measures for merchant ships, seaports and the international supply chain included amongst others;

- The International Maritime Organization (IMO)
- The International Labour Organization (ILO)
- The World Customs Organisation (WCO)[3]
- The Organisation for Economic Co-operation and Development (OECD) Maritime Transport Committee,[4] and
- The United Nations Economic Commission for Europe (UNECE)[5]

Of these efforts, the regulations that were eventually developed by the IMO have had the most impact on merchant shipping. In developing and adopting the International Ship and Port Facility Security (ISPS) Code and other security measures in amendments to the 1974 Safety of Life at Sea (SOLAS) Convention, the IMO sought to enhance the security of ships and port facilities alike. With regard to ships, the measures are meant to protect ships as 'targets' of acts of terrorism as well as to prevent their use as 'weapons' in acts of terrorism. The IMO and the ILO also worked together in an effort to further enhance port security by producing a Code of Practice addressing security in ports.[6]

THE SSAS REGULATIONS

The requirement for merchant ships to be equipped with Ship Security Alert Systems (SSASs) is found amongst the amendments made to the 1974 SOLAS Convention. The amendments were adopted in London by a Conference on Maritime Security at the International Maritime Organization in December 2002.[7]

[3] IMO Conference Resolution 9 adopted on 12 December 2002 'Enhancement of security in co-operation with the World Customs Organization')
[4] http://www.oecd.org/document/53/0,3343,en_2649_34367_2088757_1_1_1_1,00.html
[5] One example of UNECE initiatives is the meeting that was held jointly with the World Customs Organization (WCO) in Geneva on 13 and 14 November 2003 on trade security and trade facilitation.
[6] Security in Ports. ILO and IMO code of practice, 92-2-115286-3 (ISBN), This code of practice, developed jointly by the ILO and the IMO, provides useful guidelines that offer a framework for formulating and implementing security strategies and identifying potential risks to a port's security. It outlines security roles, tasks and measures to deter, detect and respond to unlawful acts against ports serving international traffic, and may also form the basis for security strategy in domestic ports.
[7] International Maritime Organization (IMO) Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974. IMO document SOLAS/CONF.5/32 12 December 2002; Consideration and Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974 , Conference resolution 1 and related amendments to the 1974 SOLAS Convention. Annex, Regulation 6 Ship Security Alert System, pages 11 and 12.

The scope of the SSAS requirements

The amendments to the SOLAS Convention require all ships to be provided with a Ship Security Alert System, fitted according to a strict timetable which required most merchant vessels to be fitted by 2004 and the remainder by 2006.[8]

When activated, the Ship Security Alert System shall initiate and transmit a ship-to-shore security alert to a competent authority designated by the ship's Administration (hereafter referred to as the 'Flag State'), including only three details; the identity of the ship, the ship's location, and an indication that the ship is under threat or that its security has been compromised.[9]

The SSAS is a silent alarm. It will not raise any alarm on board the ship. There must be at least two 'activation points' or buttons, one must be on the navigation bridge and the others are to be situated in at least one other location on the ship.[10]

The Flag States decide who will be the initial recipients of the security alerts from ships. The recipient may be one or more parties designated by the Flag State as competent authorities, which may include the Company (ship owner).[11]

Flag States' Response to SSAS on Receipt

The SSAS requirements for the Flag States stipulate that when a Flag State receives notification of a ship security alert, that Flag State shall immediately notify the Coastal State(s) in the vicinity of which the ship is presently operating. Furthermore, when a Country which has ratified the SOLAS Convention that is not the Flag State receives notification of a ship security alert from a ship, that Country shall immediately notify the ship's Flag State and, if *appropriate*, the Coastal State(s) in the vicinity of the ship.[12]

All countries that have ratified the SOLAS Convention are required to inform the IMO of the names and contact details of those parties who have been designated to be available at all times to receive and act upon the ship-to-shore security alerts.[13] This information is publicly available from the IMO Website.

NATIONAL REQUIREMENTS

There is quite a bit of flexibility built into the SOLAS maritime security measures, and this is also true regarding SSASs.

---

[8] *ibid*
[9] *ibid*
[10] *ibid*
[11] *ibid* section 6.2.1
[12] *ibid*
[13] Regulation 13 Communication of information IMO Document SOLAS/CONF.5/32 12 December 2002 CONFERENCE OF CONTRACTING GOVERNMENTS TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 Agenda item 6 CONSIDERATION AND ADOPTION OF AMENDMENTS TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 Conference resolution 1 and related amendments to the 1974 SOLAS Convention

This flexibility has enabled Flag States to take quite a number of different approaches to the management of SSAs, some requiring that only one party receives the alert, whilst others require that two or more parties are informed. The actions taken subsequent to the receipt of an alert also vary significantly amongst the Flag States.

These observations were made during a review of the procedures followed by the following 15 Flag States; the Bahamas, China, Denmark, Greece , Hong Kong, SAR, Liberia, Malta, the Marshall Islands, North Korea, Panama, Singapore, St. Kitts & Nevis, the Netherlands, the United Kingdom and the United States. Additional information describing the procedures in place with these countries is available in the Annex to this paper.

During the review it was observed that there are significantly varied systems and procedures used amongst these Flag States. Whilst there was more information available for some States than for others, for each Flag State named it was possible to identify the recipients of Ship Security Alerts. For some, more detailed information regarding the management of security alerts has been obtained in addition to indications regarding how an appropriate response would be mobilized.

Whilst this overview is by no means an exhaustive comparison, the information that has been gathered is sufficient to draw several subsequent conclusions that in turn form the basis of several recommendations.

Furthermore, the procedures followed by the ten Flag States having the world's most registered tonnage are included in this study.[14] These are;

1. Panama (146 million registered gross tones)
2. Liberia (63 million registered gross tones)
3. Bahamas (41 million registered gross tones)
4. Singapore (31 million registered gross tones)
5. Greece (31 million registered gross tones)
6. The Marshall Islands (31 million registered gross tones)
7. Hong Kong, SAR (30 million registered gross tones)
8. Malta (23 million registered gross tones)
9. China (23 million registered gross tones)
10. The United States (20 million registered gross tones)

Therefore, it is reasonable to assume that the observations made in this paper are true for a large proportion of the world's merchant fleet relating to the management of ship security alerts.

Perhaps of greatest concern is the fact that few, if any, of the flag states have systems in place that facilitate the requirement to immediately notify the nearby Coastal State(s) upon the receipt of a ship security alert. Considering that it has been shown that acts of terrorism are executed swiftly, with little or no warning, what we see with

[14] Based on information made available on the website www.shippingfacts.com, developed by the Round Table of international shipping associations (BIMCO, Intercargo, ICS/ISF and Intertanko) with the support of ECSA and OCIMF as part of a co-ordinated effort to present maritime transportation in a positive light. The ranking is based on information published by Lloyd's Register Fairplay and is based on the millions of gross tonnes of shipping registered in the countries listed.

the handling of ship security alerts is a series of steps which precede the notification of any authorities in the vicinity of the ship and thereby hinder the notification of the Coastal State(s).

Table 1

Flag State	**Initial alert recipient(s)**	**Alert validation**	**Stakeholders involved with response management** (more detailed descriptions are found in the Annex)
Bahamas	Company Security Officer (CSO)	Yes, by CSO	Bahamas Maritime Authority, London
China			Ministry of Communications, China Maritime Search and Rescue Center (CNMRCC)
Denmark	The shipowner and the Danish Navy	Yes, by CSO	Cross-agency task force including; Foreign Ministry, the Department of Defense, the Security and Intelligence Service, the Maritime Administration, as well as others
Greece	Shipowner		Ministry of Mercantile Marine Joint Rescue Coordination Center, Piraeus
Hong Kong, SAR	The shipowner and the Maritime Administration		Marine Department, The Government of the Hong Kong Special Administrative Region, Marine Rescue Co-ordination Centre (MRCC), Duty Officer
Liberia	The shipowner and the Flag State	Yes, by CSO	Office of the Deputy Commissioner for Maritime Affairs c/o the Director of Maritime Security, Liberian International Ship and Corporate Registry.
Malta	The shipowner		Malta Maritime Authority, Merchant Shipping Directorate
Marshall Islands	The CSO (or an approved third party) and the Flag State	Yes, by CSO	An Incident Contingency Plan will be initiated involving: the US Department of State Operations Center, the USCG Headquarters Command Center, the IMB, the national authority of the nearest coastal state, and the Marshall Islands Ambassador to Washington, DC.
North Korea			Maritime Security Division of the Maritime Administration Bureau in Pyongyang
Panama	The shipowner		Maritime Security Department at the Panama Maritime Authority
Singapore	Maritime and Port Authority of Singapore (MPA) Port Master's Office	Yes, by CSO	If ship in Singaporean waters: Singaporean maritime security agencies including the Police, the Coast Guard and the Navy Outside Singapore waters: The MPA contact the respective nearby Coastal States' security forces via the Marine Rescue Coordination Centers
St. Kitts & Nevis	The CSO (or an approved third party) and the Flag State	Yes, by CSO (or an approved third party)	The Director of Maritime Affairs, CSO, the St. Kitts & Nevis Coast Guard and the coastal state.
The Netherlands	The Dutch Coast Guard, however this can be done via the CSO.		The Dutch Coastguard and Navy.
United Kingdom	The CSO (or an approved third party), the Flag State and the Coast Guard at Falmouth	Yes, by CSO	Coast Guard at Falmouth, UK Department for Transport, Transport Security and Contingencies (TRANSEC) Maritime Security Branch, Metropolitan Police Service (MPS) Counter Terrorist Command (SO15), UK Cabinet Office
United States	US Coast Guard Commander Pacific Area, US Coast Guard Rescue Coordination Center (RCC) in Alameda, California	Yes, by CSO, port agent*, or local port authority.* *for US ships in US waters.	US Coast Guard Commander Pacific Area, US Coast Guard Rescue Coordination Center (RCC) in Alameda, California, the Commandant Duty Officers at the USCG National Command Center, the CG Operational Commander for the Atlantic Area or the Pacific Area (depending on the ship's location), **US Maritime Operational Threat Response (MOTR) process**, the details of which are classified, several government agencies would come together to decide the appropriate action in a timely manner. The lead may shift from one agency to another during the response. For

Flag State	Initial alert recipient(s)	Alert validation	Stakeholders involved with response management (more detailed descriptions are found in the Annex)
			example, a piracy incident may shift from the Navy to the Department of Justice

As Table 1 shows, in most cases the first step taken is for the shipowner to verify that the alert is real. This is due to a high frequency of false alerts sent from ships which is addressed later in this paper. Whilst the shipowner seeks confirmation from the ship, the Flag State is either completely unaware that an alert has been issued or is waiting for the confirmation. This initial stage of the process could take time to complete, during which time no one in the vicinity of the ship has any knowledge of a potential terrorist act underway.

After the alert has been verified, the Coastal States are still not necessarily notified immediately. Again, Table 1 indicates that several Flag States will first convene discussions amongst two or more agencies to determine what action to take. As the number of stakeholders involved in such discussions increases, the time required to reach a consensus may also be expected to increase.

Whilst it may be true that the need for expediency is of lesser concern regarding ships compromised by terrorists on the high seas, perhaps far from their intended targets, for ships positioned near highly populated areas, critical infrastructures or alongside large passenger ships, expediency is of the utmost importance if there is to be any hope of saving lives.

Use of the SSA

Resistance and concerns of seafarers and shipowners

In February 2004, only four months before the ISPS Code was to take effect, Captain Ralph Juhl, Director of Safety & Quality at Tesma Holding, Denmark, raised the question, "Do I dare activate the SSAS?"[15] This question reflected the uncertainties regarding what consequences activating the SSAS would create. Of the concerns raised, those which best illustrate why seafarers and ship owners were anxious related to who would respond to the alert, and how they would respond. The potential types of responses were assumed to differ greatly, for example between a ship far from a coastline navigating in international waters as compared with a ship situated close to a densely populated coastal or port city. In the latter case, there were (and perhaps still are to a degree) concerns that the authorities' response will be to eliminate the threat as quickly as possible, placing priority on protecting the local population with less concern for the people on board the ship.

One may recall that following the 11 September attacks there was a public debate regarding whether passenger aircraft could or should be shot down if it appeared that they were to be used as 'weapons'. Seafarers surely were not reassured by such

[15] From the presentation "Viewpoints from the bridge" made by Captain Ralph Juhl, Director of Safety & Quality at TESMA Holding during the 2nd Annual TANKEROperator Conference, London, 3 & 4 February 2004

considerations whilst the Ship Security Alert Systems were being installed on their ships.

Other concerns remain today. One industry contact feels that Ship Security Alert Systems are almost useless as they provide no indication regarding the nature of the security threat faced by the ship activating the alarm. In the absence of such details, how can shore side authorities plan an appropriate response?

The actual use of SSASs

There were no examples of acts of terrorism found involving merchant ships that took place after Ship Security Alert Systems became mandatory. However, one recent act of terrorism involving a merchant ship raises some questions regarding the benefits of SSASs.

On 6 October 2002 the tanker LIMBURG was attacked by terrorists off the Yemeni coast. A small unmanned motorboat loaded with explosives was maneuvered at high speed alongside the tanker and detonated. The ship's hull was penetrated causing environmental consequences as the cargo of oil was spilled and a fire ensued. One of the crew died.

Considering the speed with which this attack was carried out, even if there had been an SSAS installed and activated as soon as the motorboat was spotted, it is not likely that any responders could have done anything to prevent the incident.

Finally, the button is pushed

It is difficult to establish exactly when the first SSA was sent during an actual security incident. The early reports from July 2004 onwards primarily cite human error and other mishaps when testing the SSASs, during which time there were troubling anecdotes circulating. Most alarming was an account of an alert being issued in error (the 'live' button was pressed instead of the 'test' button). Despite the fact that the system is designed to be a covert alarm,[16] on receipt of the alert the coastal state's authorities made direct contact with the ship. This indicated that the authorities which received the alert were unaware of the procedures stipulated in the internationally agreed regulations, and thereby defeated the purpose of the 'silent' nature of the alarm.

The first correct use of the SSAS was not in connection with an act of terrorism but rather with regard to the much more prevalent scourge of piracy. Looking at reports published by the ICC/International Maritime Bureau[17] and the ReCAAP Information Sharing Centre[18] during 2006 and 2007, there is an increased frequency of reports

[16] International Maritime Organization (IMO) Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974. IMO document SOLAS/CONF.5/32 12 December 2002; Consideration and Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974 , Conference resolution 1 and related amendments to the 1974 SOLAS Convention. Annex, Regulation 6 Ship Security Alert System, pages 11 and 12.
[17] http://www.icc-ccs.org/prc/piracyreport.php
[18] http://www.recaap.org/

showing that crew are activating the Ship Security Alert Systems when faced with piracy and armed robbery.

Advice received from a Norwegian Company Security Officer indicates that SSASs are sometimes only part of the procedures implemented on board when ships face security risks. This is explained in view of the current deployment of Naval Ships, Marine Police and Coastguards in sensitive areas. Therefore ships are encouraged to contact the IMB or other agencies such as MARLO[19] and the NATO Centre directly for assistance, whilst simultaneously activating the SSAS.

If time and circumstances permit, merchant ships can (and do) contact Naval ships directly for assistance using VHF Channel 16. Naval assistance has also been obtained by ships which have contacted the IMB Piracy Reporting Centre in Kuala Lumpur, who in turn contacts either MARLO or NATO. Ships and CSOs have also appealed directly to MARLO and NATO for assistance.

MARLO's mission is to facilitate the exchange of information between the United States Navy and the commercial shipping community in the U.S. Central Command's area of responsibility. MARLO, situated in Bahrain, is also committed to assisting the commercial shipping community. The MARLO staff is made up of combination of US Coast Guard, US Navy, and civilian personnel.

Ships that wish to seek assistance directly from NATO can do so in various ways, one of which is by contacting the NATO Shipping Centre in Northwood UK via toll-free telephone lines or email. By providing available information regarding the assumed threat and other details such as the ship's course and speed, position, and description of the suspicious vessel(s), the Shipping Centre can then determine which NATO assets are nearby for deployment.[20]

The DANICA WHITE

In the course of this study only one case has been identified in which the SSAS was the only means used to obtain assistance. The result was not impressive.

The incident took place on 1 June 2007 on board the Danish vessel DANICA WHITE. She was boarded by pirates 205 miles off the Somali coast. The ship had not posted a watch, hence the pirates were not noticed until they were on board the ship, taking everyone on board by surprise. As the pirates stormed the bridge the ship's Captain only had time to press the button on the SSAS. Having done so he assumed that the security alert had been sent to the Danish Navy's headquarters in Denmark.

Unfortunately there is no record of the alert being received by the Danish Navy. Subsequent testing of the SSAS equipment on board the ship found no signs of any faults with the equipment, so the reason for the failure remains a mystery.

In the meantime the US Naval ship USS CARTER HALL was nearby and observed the suspicious activity on board the DANICA WHITE. The CARTER HALL

[19] Maritime Liaison Office (MARLO) Bahrain www.marlobahrain.org
[20] Based on information received from a Norwegian Company Security Officer and the NATO Shipping Centre website http://shipping.manw.nato.int

contacted the DANICA WHITE by radio and was informed of the piracy situation. Attempts were then made to prohibit the DANICA WHITE from entering Somali waters, including the firing of flares and warning shots across the bow. Three motorboats belonging to the pirates which were in tow were fired upon and destroyed. Despite such actions the DANICA WHITE was able to enter Somali waters. The CARTER HILL then held her position and observed the situation.

During these events the USS CARTER HILL was able to make contact with the owners of the DANICA WHITE based in Denmark. The owners were unaware that the SSAS had been activated. After checking with the ship broker the owners were able to inform the USS CARTER HILL that the DANICA WHITE had no business to conduct in Somalia, thereby verifying that she was now under control of the pirates. Eventually negotiations were arranged with the Somali captors and once a ransom was paid the ship and her crew was released after 83 days of captivity.

The DANICA WHITE case, the only one identified in which the SSAS was the sole means used to seek assistance in the face of a security threat, leaves little confidence in the ability of the system to generate a rapid response, much less with respect to preventing acts of terrorism.

Other ships that faced security threats have been successful in acquiring assistance without using the SSAS but rather by conventional means.

DAI HONG DAN

The North Korean cargo ship DAI HONG DAN was attacked by Somali pirates on 29 October 2007.

When the DAI HONG DAN was boarded by Somali pirates who took control of the bridge, the crew was able to maintain control of the steering gear and engine room. The crew also managed to inform the ship owner of the situation on board.

The ship owner then contacted the Korean authorities, most likely the Maritime Security Division of the Maritime Administration Bureau in Pyangyang. Subsequently the Korean embassy in London contacted the ICC/International Maritime Bureau (IMB).

The IMB in turn phoned the Combined Maritime Forces Headquarters, based in Bahrain, on the morning of 30 October 2007. [21]

According to information received from the US Navy, the US 5th Fleet was notified at 05:39 hours on 30 October 2007. At that time the US Navy destroyer USS JAMES E. WILLIAMS was about 50 nautical miles from the Dai Hong Dan. She was ordered to proceed to the DAI HONG DAN and escort and assist her. The struggle between the pirates and the crew to control the ship continued as the USS JAMES E. WILLIAMS approached. At 06:38 the crew reported that one crewmember had suffered a gunshot wound.

[21] This sequence of events is based on several media reports including articles found in Lloyd's List, CNN,com, the International Herald Tribune, US Navy website and interviews with the IMB.

At 07:57 a helicopter was sent from the USS JAMES E. WILLIAMS to investigate the situation on the DAI HONG DAN. No activity was observed by the helicopter crew. At 08:50 bridge to bridge communication was established with the pirates, who agreed to surrender once the USS JAMES E. WILLIAMS arrived. Further discussions took place at 11:55 hours, when the pirates agreed to throw their weapons overboard and surrender to the North Korean crew.

During the earlier gun fight one pirate was killed, and critical injuries were sustained by three pirates and three crew. Three other crew suffered lesser injuries. All were treated by the US Navy boarding team that boarded the ship at 13:25.[22]

Three aspects of the DAI HONG DAN incident are worthy of note; The first is that this is the only documented contemporary case in which the crew killed a pirate. The second is that diplomatic tensions between the United States and North Korea did dot prevent the US Navy from coming to the aid of a North Korean merchant vessel. Lastly, it shows that a rapid response can be attained without use of the SSAS.

SEABOURN SPIRIT

The SEABOURN SPIRIT has been involved in two incidents in which alternatives to the SSAS were utilized in the face of security threats.[23]

The first took place off Somalia on 5 November 2005. Somali pirates in motorboats fired machine guns and rocket propelled grenades at the ship in an effort to get her to stop so they could board. To prevent the attackers from boarding the Captain initiated evasive maneuvers as recommended in the IMO guidelines. A Distress Alert was sent to the Marine Rescue Coordination Center (MRCC) in Stavanger, Norway.

The Stavanger MRCC then informed IMB Piracy Reporting Center in Kuala Lumpur, which immediately contacted coalition forces operating in the area. In this case the role and the action taken by the IMB could be described as that of an international response coordinator. In the meantime the SEABOURN SPIRIT continued her evasive actions and used acoustic defense equipment. The attackers then aborted their pursuit. Afterwards the US Navy provided assistance in removing an unexploded grenade that was wedged in the wall of a cabin.

The second incident involving the SEABOURN SPIRIT took place off Oman in November 2007. Here suspicious craft were spotted in the ship's vicinity. In this case the
United Kingdom Maritime Trade Organisation (UKMTO) received the distress call and immediately informed the United Kingdom's Maritime Component Command (UKMCC). The UKMCC in turn contacted HMS CAMPELTOWN which dispatched a helicopter to assist. As the helicopter arrived at the scene the small boats left the area.

[22] The details of the sequence of events on board the DAE HONG DAN were kindly provided by USN CDR Lynn "Mulan" Chow, Executive Assistant, Commander, US Naval Forces Central Command
[23] The details of these attacks have been culled from various reports issued by the IMB, published by Lloyd's List, and information provided by the US Offoce of Naval Intelligence and USN CDR Lynn "Mulan" Chow, Executive Assistant, Commander, US Naval Forces Central Command

Shortcomings of SSASs and advantages of other options

The incidents involving the DANICA WHITE, the DAI HONG DAN, and the SEABOURN SPIRIT, although only a handful of the hundreds of incidents experienced annually, each respectively illustrate the shortcomings of the SSAS, the advantages of engaging an international response coordinator and the advantages of alerting rapid responders directly.

One lesson learned from the DANICA WHITE case is that for the time being, the security alert systems are not reliable enough to be considered as a sole means for acquiring assistance. Despite the Captain's effort to activate the alert system, there is no trace of the alert being received by the Danish Navy. A second lesson learned regards the value of having naval forces present in high-risk areas, as the crew of the USS CARTER HILL took action as soon as they suspected that there was a security breach on the DANICA WHITE.

The DAI HONG DAN case shows that when the crew is able to contact the ship owners and give a detailed description of the security threat, such information can be channeled to a party acting as an international response coordinator, in this case the IMB, who in turn can rely upon established connections to expedite a rapid response to assist the ship.

The two incidents involving the SEABOURN SPIRIT again did not include use of the ship security alert system, but rather show the advantages of contacting response coordinators. Whilst the 2005 incident, like that of the DAI HONG DAN, illustrates how an international response coordinator, again the IMB, can facilitate the mobilization of response forces, the 2007 incident shows that the responders themselves can be contacted directly for assistance, in this case the Royal Navy.

False alerts

Since the introduction of SSASs there have been many incidents of false alerts. Whilst no official statistics have been compiled, the frequency of false alerts was high enough to warrant discussions at the IMO during the 78th session of its Maritime Safety Committee in May 2004.[24]

Even though there are no comprehensive statistics available, information provided by the US Coast Guard and the Danish Navy[25] indicate that there are potentially thousands of false alerts sent annually, even towards the end of 2007. This conclusion is drawn from the fact that the US Coast Guard alone received more than 100 false

[24] IMO MSC Circ. 1109/Rev.1 False Security Alerts and Distress/Security Double Alerts dated 14 December 2004

[25] The number of false security alerts received as provided by the US Coast Guard on 30 November 2007:
Oct 2005 to September 2006; 60 false SSAs received
Oct 2006 to September 2007; 120 false SSAs received
Since 1 October 2007; 24 false SSAs received
The number of false security alerts received as provided by the Danish Navy:
2004; 25 false SSAs received
2005; 10 false SSAs received
2006; 24 false SSAs received

alerts in fiscal year 2007. As the US is only the world's tenth largest ship registry, one could assume that an equal or higher number of false alerts is received by the world's nine larger registries, which together are responsible for four times the amount of merchant shipping tonnage as compared with the US.

Sadly, one 'real' alarm that the DANICA WHITE attempted to send to the Danish Navy was not received.[26]

The high frequency of false alerts has detrimental consequences. Of these perhaps the most grave is that this can lead to complacency amongst those regularly receiving false alerts, an effect similar to that experienced by the villagers in Aesop's fable of the boy who cried wolf. Such complacency will reduce the likelihood that immediate action will be taken to mobilize a rapid response to a real alert.

Another consequence resulting from the high frequency of false alerts is that many Flag States now require that all alerts received are verified before any actions are taken to organize a response. Whilst this does reduce the amount of time and resources that would be wasted when responding to false alerts, it does not serve well to ensure the most rapid response possible.

Information received from Securewest International, which is an approved competent authority for several Flag States, indicates that it is possible to effectively reduce the frequency of false alerts.[27]

Securewest has informed the author that after engaging thier services as the competent authority for the receipt of security alerts, one shipowner improved their proper security alert verification from 30% to almost 75%, with over 95% of their ships being able to properly reset the equipment after testing. Whilst such improvements are admirable, they do show that much work lies ahead if false alerts are one day to be completely eliminated.

Regional Arrangements

As seen in the description of National arrangements for SSAS management, there are circumstances in which Flag States must work with other nations and other stakeholders in order to arrange for timely and effective responses to SSAs.
This leads to the question; Are there any regional arrangements already in place that could facilitate such responses to SSAs? Obviously there are regional and international cooperative arrangements between nations relating to a multitude of issues. Which of these, if any, could have advantages for the management of SSAs?

---

[26] As indicated in the report published by the Danish Maritime Authority's Divsion for Investigation of Maritime Accidents dated 16 November 2007 and stated by the Captain of the DANICA WHITE Niels Henze Nielsen in an interview that appeared in the Danish newspaper Berlingske Tidende on 2 September 2007 "DANICA WHITE var et let offer" Domestic News page 10 (free translation; DANICA WHITE was an easy target)

[27] Paul Singer, Vice President (Business Development) of Securewest International kindly provided this information to the author. UK Office +44 (0)1548 856001, Facsimile +44 (0)1548 857641 URL www.securewest.com

The European Union

Some 'regions' would appear to be ripe for the coordination of SSA response. The European Union (EU) would appear to be well suited for such coordination with 27 member states (MS), many of which have rich maritime histories, are Coastal States and are home to ship owning and managing companies.

However, presently the only harmonization with respect to SSASs is limited to a requirement that EU MSs report to the European Commission to confirm that they have systems in place to manage SSAs.

Mr. Christian Dupont, Deputy Head of Unit and Policy Officer at the European Commission's Directorate of Transportation and Energy explains the European requirements as follows; "The European legislation requires MSs of the EU to have in place a system whereby SSAS are received and processed for ships flying their flags, and to report to the European Commission that this system is in place. The existence of such systems and their relevance 'on paper' is verified during the Commission's inspections in national administrations of MS.

But this is where the Commission's mandate stops.

The practical arrangements are left up to each MS, as there is no real "operational" external policy of the EU (unless unanimity is reached amongst the 27 MSs) and in particular in this very narrow and specialized field, each MS would, for the time being, be more efficient in activating its own diplomatic channels to react to an SSA sent by one of its flagged ships in another part of the world, unless it knows that it can ask for assistance of a war ship of another EU MS in the surrounding area if the event happens in international waters.

Furthermore, the organization of maritime administrations differs largely from one MS to another; therefore SSAs are received in different ways depending on the flag."

Although no formal mechanism has been established amongst the members of the EU, in practice they, just like nations in other regions, could turn to other regional arrangements when managing SSAs.

A report published in Jane's on 12 November 2007 indicates that Europe's Navies are moving towards coordination involving NATO and other stakeholders. The report states that a consensus is emerging across Europe that the EU needs a coordinated maritime security policy enabling navies to work far more closely with national and EU law-enforcement and counterterrorism agencies than in the past.[28]

Policy makers from both the EU and NATO stress, however, that more effective maritime security depends less on new equipment and capability and more on achieving tighter co-operation and interoperability between maritime players within each nation and in co-ordination with EU and NATO agencies.[29]

---

[28] *Europe focuses on better co-ordinated maritime security* by Brooks Tigner, article dated 12 November 2007 available from Jane's, *http://www.janes.com/*

[29] *ibid*

"For the first time all nations now agree that the maritime environment must become a controlled one similar to air space," Vice Admiral Ferdinando Sanfelice di Monteforte, Italy's military representative to the EU and NATO, told a half-day conference organised on 8 November 2007 by the Security and Defence Agenda think-tank.[30]

Noting that Italy's navy welcomes and uses situational awareness information from all Mediterranean 'blue water' and littoral forces, whether NATO or EU, he said the new consensus "is a big shift in thinking and there is a proven willingness among our navies to work together."[31]

Vice Admiral Anthony Dymock, UK military representative to NATO and EU, agreed. "There are encouraging signs that navies, national civil maritime security authorities and EU agencies such as the European Defense Agency are making progress," he said. "This isn't navies just looking for a new role... most navies now recognize that we cannot do it all ourselves, and that the primary lead has to come from civilian actors."[32]

ADM Dymock said: "We need a formal process to better define responsibilities and to share information such as satellite imagery and intelligence, which probably requires a new Memorandum of Understanding among participating nations."[33]

With many stakeholders in Europe now conscious of a need to coordinate their activities in respect of maritime security, there may be opportunities to establish a regional mechanism that would streamline the handling of ship security alerts transmitted by ships in European waters. Having one central coordinating point capable of mobilizing responders nearby would be advantageous in accelerating appropriate rapid responses. There may even be a role for the European Maritime Safety Agency to play as an advisor, facilitator or coordinator.

Asia

The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) was finalized on 11 November 2004 in Tokyo, and came into force on 4 September 2006. It is the first multi-lateral government-to-government response of its kind that addresses the challenge of piracy and armed robbery in the context of the ASEAN+6 countries.[34]

The origins of ReCAAP go back to a series of initiatives that began with the Asia Challenge Conference in 2000 at which the Japanese government called for government organizations and law enforcement agencies to jointly address the increasing trend of crimes at sea. Two documents emerged out of that conference; the Tokyo Appeal and the Model Action Plan. These two documents, which reiterated the

[30] *ibid*
[31] *ibid*
[32] *ibid*
[33] *ibid*
[34] From the presentation "The Roles of the ReCAAP ISC" delivered by ReCAAP Executve Director, Mr Yoshiaki Ito and Mr. Ranjeet Singh, ReCAAP Research Manager at the 6th ICC-IMB Tri-Annual Meeting on Piracy and Maritime Security, Kuala Lumpur, 12-13 June 2007

IMO Maritime Safety Committee Circulars 622[35] and 623[36], were fundamental in laying the foundation for adopting a multi-lateral approach to piracy and armed robbery.

In 2001 a further step was taken when the former Japanese Prime Minister Koizumi Junichiro mooted the concept of a regional agreement among governments to address the growing concern. This set the stage for drafting of the ReCAAP Agreement by sixteen countries that include the People's Republic of Bangladesh, Brunei Darussalam, the Kingdom of Cambodia, the People's Republic of China, the Republic of India, the Republic of Indonesia, Japan, the Republic of Korea, the Lao People's Democratic Republic, Malaysia, the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Democratic Socialist Republic of Sri Lanka, the Kingdom of Thailand, and the Socialist Republic of Viet Nam.[37]

Under the ReCAAP agreement each participating country establishes a Focal Point to act as the point of contact for the ReCAAP Information Sharing Center. Each Focal Point is responsible to;

1) manage incidents of piracy and armed robbery within its territorial waters
2) act as point of information exchange with the ReCAAP ISC
3) facilitate its country's law enforcement investigations
4) co-ordinate surveillance and enforcement for piracy and armed robbery with neighbouring Focal Points[38]

In the event that a SSA is issued from a ship and received by one of the sixteen ReCAAP countries, that country could benefit from the information exchange network facilitated by the ReCAAP Information Sharing Center (ISC) primarily when the victim ship is navigating within the ReCAAP region[39].

For incidents taking place within the territorial waters of a ReCAAP country, that country can be quickly contacted via its Focal Point and the respective national agencies could then be deployed.

When a ship issues an SSA whilst navigating in international waters within or nearby the ReCAAP region, the ReCAAP ISC can quickly transmit the information to several (in fact all) ReCAAP countries. The advantage being that the respective Focal Points can then take steps to determine what, if any, assets were available and of these which may be close to the vicinity of the incident. On receipt of such information from one

[35] IMO Maritime Safety Committee Circular MSC/Circ.622/Rev.1 dated 16 June 1999 "PIRACY AND ARMED ROBBERY AGAINST SHIPS Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships"
[36] IMO Maritime Safety Committee Circular MSC/Circ.623/Rev.3 dated 29 May 2002 "PIRACY AND ARMED ROBBERY AGAINST SHIPS Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships"
[37] From the presentation "The Roles of the ReCAAP ISC" delivered by ReCAAP Executve Director, Mr Yoshiaki Ito and Mr. Ranjeet Singh, ReCAAP Research Manager at the 6th ICC-IMB Tri-Annual Meeting on Piracy and Maritime Security, Kuala Lumpur, 12-13 June 2007
[38] *ibid*
[39] Should a ship be navigating outside the ReCAAP region, the ReCAAP ISC may still be able to help by contacting its international counterparts such as the ICC/International Maritime Bureau or the IMO.

or more Focal Points the ReCAAP ISC would be in a position to facilitate the further exchange of information.

ReCAAP incident response in practice

Contacts at ReCAAP report that there have been cases in which CSOs have contacted the ReCAAP Focal Points directly on receipt of SSAs. During the first eleven months of 2007 there were 4 such incidents. In these cases, the ReCAAP Focal Points took the necessary measures such as dispatching response units to the ships that requested assistance, alerting law enforcement agencies, and finally issuing the Incident Reports to the ReCAAP ISC and the other Focal Points.

In such cases the reports were received by the ReCAAP ISC after the attacks were over.

ReCAAP anticipates that the ISC will generally receive the reports post-attack, with certain exceptions such as hijackings or kidnappings.

This is consistent with the present role of the Focal Points and the ReCAAP ISC. Currently the ReCAAP ISC has no authority to render operational assistance to the victim ship; however, being an information sharing centre, on receipt of a 'live' alert, the ISC could subsequently inform the nearest Focal Points about the incident so that assistance could be provided.

Amongst other initiatives taken in Asia is the establishment of the Changi Command and Control Centre in Singapore which will unite the Singapore Maritime Security Centre, the Information Fusion Centre and the Multinational Operations and Exercises Centre all under one roof, to sustain a high level of coordination against maritime threats. The strategy is aimed at coordinating local, regional and international efforts, and is expected to be operational in 2009. The complex will also help to facilitate greater cooperation among the security agencies of international and regional governments to deal with threats like piracy and terrorist attacks on ships. [40]

Africa

Ships attacked by pirates off the Somali Coast have received assistance from naval ships participating in Combined Task Force (CTF) 150, which is one of three task forces under Combined Maritime Forces, a 20-nation Coalition based in Manama, Bahrain.[41]

According to information made available by the US Navy, the waters off Somalia and the Horn of Africa are part of the area under the responsibility of CTF 150. A key mission of the Coalition is conducting Maritime Security Operations (MSO), which help set the conditions for security and stability in the maritime environment and complement the counterterrorism and security efforts in regional nations' littoral waters. Coalition forces also conduct MSO under international maritime conventions

[40] Straits Times, 28 March 2007, *3 Maritime Centres To Be Under One Roof*
[41] US Navy website article "UPDATE: Crew of North Korean Pirated Vessel Safe" dated 30 October 2007 http://www.cusnc.navy.mil/articles/2007/226.html

to ensure security and safety in international waters so commercial shipping and fishing can occur safely in the region.[42]

The Coalition includes representation from Australia, France, Germany, Italy, Pakistan, the U.K. and U.S., as well as naval forces and personnel from several other nations. Coalition ships patrol more than 2.5 million square miles of international waters.[43]

In addition to its involvement with CTF 150, the US Navy is also conducting operations within African waters under a new unified U.S. military command for the continent called Africom that commenced operations in November 2007. This operation will not only serve to raise the profile of naval forces in these waters but will also involve training exercises for African Navies.[44]

A similar US Navy supported initiative is the Africa Partnership Station (APS). APS is one in a series of activities designed to build maritime safety and security in Africa in a comprehensive and collaborative manner, focusing first on the Gulf of Guinea. It responds to specific African requests for assistance, is aligned with broad international community and U.S. objectives, and is reflective of the mission of the U.S. Africa Command . It seeks to take partnerships into action in a concerted interagency and multinational effort to promote maritime governance around Africa. APS is inspired by the belief that effective maritime safety and security will contribute to development, economic prosperity, and security ashore.[45]

Another initiative has been taken by the Maritime Organization for West and Central Africa (MOWCA) which met in September 2007 to discuss ways to establish an African Coast Guard network aimed at the establishment of coordinated coastal patrols. A key goal in putting such a system in place is to be able to quickly respond to piracy and armed robbery attacks.[46]

Americas

There is a degree of regional cooperation in the Americas.

Canada invited American participation with its operation dubbed “Exercise Sea Barrier”. First conducted in February 2005, the exercise was designed to test co-operation between many Canadian agencies responsible for securing Canada's Pacific maritime approaches, and took place in the Juan de Fuca Strait area off Canada's west coast.[47]

---

[42] *ibid*
[43] *ibid*
[44] As reported by the Associated Press on 7 November 2007 and circulated by the US Maritime Security Council MSC ALERT. www.maritimesecurity.org
[45] From reports published on www.cnn.com and the USN APS website www.c6f.navy.mil/APS
[46] As reported in Lloyd’s List on 12 October 2007 *IMO asked to take stronger action against pirates and support African coastguard* by Craig Eason
[47] From the article *Canadian maritime exercises test co-operation* by John Hill that appeared in Jane’s on
23 March 2005 www.janes.com

Contributing to the exercise were vessels, air assets and personnel from the Canadian Forces; the Royal Canadian Mounted Police (whose West Coast Marine Detachment operate four high-speed patrol catamarans, as well as rigid-hulled inflatable boats), the Coast Guard, and the Canadian Border Services Agency (which has a specialist boarding team that focuses on pleasure craft operating mainly around the San Juan Islands). Transport Canada and the US Coast Guard also took part.[48]

In testing inter-agency co-operation in combating non-military maritime threats, such as the movement of illicit drugs, illegal migrants, and terrorist activities, the exercise reflects a significant change in Canadian national security concerns. Commander Darren Hawco, whose department organized the exercise, commented that, "The level of effort in maritime security has gone way up. This is a direct result of 9/11,"[49]

Canadian Rear Admiral Jean Yves Forcier, Commander of Maritime Forces Pacific, further explained that "Canada's National Security Policy directs the Navy to increase its on-water presence and surveillance activities. With the size of our coastline and the considerable number of ships that operate in our waters, we need to maximise cooperation and collaboration amongst all the government departments with interests in the sea as well as our American allies to make sure Canadian and international laws around our own shores are respected."[50]

"The Strait of Juan de Fuca is one of our busiest bits of ocean. Vancouver moves 66 million tonnes of cargo a year including over 1.5 million containers. Exercise Sea Barrier will enhance our ability to defend and protect our trade, and ultimately our way of life."[51]

According to the Canadian Navy's website, the exercise was conducted again in February 2006.

One would hope that the goal of maximizing cooperation and collaboration between the involved agencies has been achieved. Simultaneously it would be hoped that upon receipt of an SSA, the Directorate of Marine Security at Transport Canada (Department of Transportation)[52] will have established contacts amongst the responsible agencies that can arrange a timely and effective response, particularly for ships that have issued SSAs within Canadian waters.

International arrangements

Having considered the national and regional arrangements identified and described thus far, whilst some have proven their effectiveness, others are still in the planning stages. Several appear to be of an ad-hoc nature and involve so many parties that the goal of achieving a rapid response to prevent acts of terrorism may not be achievable.

---

[48] *ibid*
[49] *ibid*
[50] *ibid*
[51] *ibid*
[52] The agency responsible for the receipt of ship to shore Ship Security Alerts according to the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments.

Therefore it may be worthwhile to consider the potential benefits of an international mechanism for security alert response coordination. Presently there are no formalized international ship security response coordinators, however, in practice there is one body that has taken on such a role, the ICC International Maritime Bureau.

The ICC International Maritime Bureau (IMB) is a specialized division of the international Chamber Of Commerce (ICC). The IMB is a non-profit making organization, established in 1981 to act as a focal point in the fight against all types of maritime crime and malpractice. A major part of the IMB's work to make shipping safer involves assisting in the suppression of piracy and armed robbery against ships around the world. In 1992, the escalating number of piracy incidents led to the establishment of a Piracy Reporting Centre in Kuala Lumpur, Malaysia. Its job is to raise awareness of piracy hotspots, detail specific attacks and their consequences, and investigate incidents of piracy and armed robbery at sea and in port.[53]

The IMB has, on many occasions, taken on the role of an international rapid response coordinator for ships in need of assistance relating to security threats. As seen with the cases of the SEABOURN SPIRIT and DAI HONG DAN, both MRCCs and Flag State authorities have sought the IMB's assistance in mobilizing assistance for ships under attack. It should be borne in mind that these are only two examples amongst many, and others have included ships and company security officers that have made direct contact with the IMB's Piracy reporting Center in Kuala Lumpur.

The IMB has informed the author that despite its track-record of effective handling of requests from ships, the IMB Piracy Reporting Centre (PRC) is not designated by any Flag State to receive ship security alerts directly from vessels as a Competent Authority. However, in practice vessels that have the CLS/ ShipLoc SSAS on board do transmit their ship security alerts directly to the IMB PRC.

IMB's present role could be described as an ad-hoc international security alert response coordinator. Contacts at the IMB feel that the only obstacle preventing it from becoming the primary or sole international coordinator for SSAS response is funding. If the IMB had adequate funding, its Director Pottengal Mukundan has informed the author that not only would it make a lot of sense for the IMB PRC to act as an international SSA response coordinator, but the IMB would also welcome the opportunity.

Conclusions and recommendations

Many observations were made during the course of the research conducted in the preparation of this working paper. Of these, perhaps the most significant is that acts of terrorism are executed with little or no time to organize preventive or mitigating actions, therefore every second is critical.

With this in mind, the SSAS system today is unreliable and the related procedures are too slow to prevent an act of terrorism.

[53] From the ICC IMB website http://www.icc-ccs.org/imb/overview.php

The SOLAS regulations as they are now written do not take heed of the need for expediency, as the communication chain involves too many parties, and this all takes place prior to the actual responders becoming involved.

Due to the international nature of the shipping business, it is likely that the security alert is received by a party far from the location of the incident. The Flag State, the ship owners and the 'competent authority' receiving the security alert may all be situated far from the areas in which the ship is trading.

This serves only to delay an appropriate rapid response to the threat. During this process no one in the immediate vicinity is warned, therefore no one in the immediate vicinity can either respond to the threat or evacuate from it.

A distress alert will generate a more rapid response.

To correct the situation, priority should be given to informing the actual responders to a security incident as quickly as possible. Unfortunately the majority of arrangements now in place for the management of security alerts do not achieve this. The responders are only informed after the alert has been verified and is subsequently passed between a number of parties.

The SSAS can, however, be useful as a last resort if terrorists have gained control of a ship, but only if false alerts are eliminated. Activation of the SSAS must result with a rapid response, just like a fire alarm. Achieving this may only be possible if the security alert is received by nearby responders or response coordinators and there is reasonable confidence that the alert is real.

Recommendations; what can be done to make security alerts effective?

1. Accelerate the alert management process

The response time can be reduced if response management is streamlined. In the best case the responders, such as naval ships in the vicinity or shore based security forces, could be the initial recipients of the alerts. The next best option would be to have security alerts received by regional or international response coordinators who are capable of mobilizing the appropriate responders, just as they now do regarding incidents of piracy.

It would also be advantageous to inform other merchant ships in the vicinity of the imminent threat, thereby enabling them to decide whether to provide assistance or to evacuate the area. One way this could be achieved is by using ships' Automatic Identification Systems (AIS). Such systems could be modified to display that a ship had activated its SSAS. Security forces at sea and authorities on shore monitoring AIS could quickly initiate appropriate measures, such as the evacuation of nearby areas and the implementation of response measures.

2. Address the false alert problem

The current level of false alerts can create a level of complacency amongst the recipients of security alerts. In order to ensure that security alerts are taken seriously

when received and promptly acted upon it is imperative that the false alert problem is corrected as a matter of urgency. This can be pursued in a number of ways.

Efforts can be made to improve the training of crew in the usage of SSAS equipment.

Consideration can be given to redesigning SSAS equipment to enable an alert recall function.

Furthermore, the prescribed usage of security alerts could be re-examined to emphasize that activation should only be considered as a last resort in extreme security situations. If it is internationally agreed that the SSAS system should only be activated in the face of an imminent, deadly and/or catastrophic event, and only when there is no other means of alerting security authorities, misuse and improper use could be reduced significantly whilst received alerts would be taken seriously and treated with the required level of urgency.

3. Expand the amount of information sent in security alerts

The information presently contained in ship security alerts provides the recipient with no indication as to the nature or severity of the threat. Exploring ways to enhance the information sent (as has been done by Liberia) would be advantageous as it would improve the recipients' ability to coordinate an appropriate response.

4. A new strategy and focus

Instead of placing the emphasis on the SSAS as the best means available to alert shore based authorities of impending or actual breaches of security including acts of terrorism, the SSAS should be promoted as a measure of last resort. Instead of immediately activating the SSAS, seafarers should be encouraged to use traditional means of communication to obtain assistance, as has been done with VHF radio Channel 16, satellite communications and even telex and email. The key advantage is that by using these means of communication the responders will obtain details of the threat and therefore be much better placed to organize an appropriate and timely response.

5. Update the IMO Piracy Guidelines

There is no mention of SSASs in the present IMO guidelines relating to piracy and armed robbery. An effort could be made to address use of the SSAS in these guidelines to emphasize that the SSAS is only to be activated as a last resort in the most extreme situations in which loss of life is imminent. The development of guidelines specific to the use of SSAS could be initiated as well, emphasizing these same points.

6. Other areas to consider

To realize the full potential that efficiently organized security alert management could produce, there are several additional areas which could be explored.

There may be potential to further amend the IMO Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988 (SUA), initially developed to facilitate the apprehension of persons committing criminal acts against ships, to incorporate measures contracting governments could take when an SSAS is activated.

Similarly there may be opportunities to expand the scope of the Proliferation Security Initiative (PSI) such that participating countries agree to cooperate in taking appropriate actions when SSASs are activated. As the PSI signatories have agreed to cooperate in intercepting, boarding, detaining and preventing ships suspected of knowingly or unknowingly facilitating the movements of weapons of mass destruction and related components. Perhaps these same nations would be willing to establish similar levels of cooperation in responding to ships that have issued security alerts. This would seem to be an appropriate aspect to include within PSI as a ship under the control of terrorists may be likely to have weapons of mass destruction concealed on board.

Like the proposal to incorporate security alert indicators on AIS displays, there may be advantages in linking SSAS systems to Long Range Identification and Tracking equipment. In this way Flag States, Coastal States and States monitoring ships in transit would all become aware of an activated security alert system simultaneously.

The Quality Coastal State concept introduced by BIMCO and now being pursued by the European Commission in its Future Maritime Policy as a means to ensure that Coastal States are meeting their obligations under international maritime conventions could be expanded to incorporate a criterion based on Coastal States' abilities to provide appropriate rapid response to ships activating their SSAS whilst in their territorial waters. At the moment the authorities that will receive security alerts are known, however, the capacity to organize a response is not. The Quality Coastal State concept would be a useful one in assessing such capacity, and in identifying areas where capacity building initiatives are needed.

The SSAS issues a silent alarm. The benefits, if any, of using a silent security alarm may be worthy of reevaluation, as the overt nature of alarms used relating to incidents of piracy and armed robbery have proven to be advantageous a deterrent. Such attackers have abandoned their plans on the activation of overt alarms. In the meantime, the only person on a ship that will be aware of the activation of the SSAS is the person that activated it, no one else will know, therefore no one else will be able to take action or evacuate the ship. For these reasons, consideration should be given as to whether the security alert should be silent.

A closing thought

Unfortunately the benefits provided to global security and within it maritime security from the implementation of requirements for ship security alert systems are limited, if there are any to be found at all. However, by implementing small changes there is the potential that the effectiveness of these systems can be significantly enhanced.

Clearly this will require efforts on the part of governments and industry stakeholders alike. Whether such steps will be taken remains to be seen, however, if just one of the

recommendations mentioned in this paper is implemented, contributing to the prevention of a single act or terrorism, then potentially thousands of lives can be saved.

Certainly that fact alone would warrant a fresh look at the SOLAS ship security alert system requirements.

ANNEX

Flag State Ship Security Alert System Response Management Procedures

This annex provides information regarding how ship security alerts are managed for ships registered with the following Flag States:

1. Bahamas
2. China
3. Denmark
4. Greece
5. Hong Kong, SAR
6. Liberia
7. Malta
8. Marshall Islands
9. North Korea
10. Panama
11. Singapore
12. St. Kitts & Nevis
13. The Netherlands
14. United Kingdom
15. United States

For all Flag States listed it was possible to identify the recipients of Ship Security Alerts. For some, more detailed information regarding the management of security alerts has been obtained in addition to indications regarding how an appropriate response would be mobilized.

The summaries vary in depth due to differences in the amount of available information, varying degrees of cooperation from Flag States and time constraints. Whilst this overview is by no means an exhaustive comparison, the information that has been gathered is sufficient to draw several conclusions that in turn form the basis of the working paper's recommendations.

Bahamas

The SSAS requirements of the Bahamas Maritime Authority (BMA) stipulate that Company Security Officers are the initial recipients of SSAs, and that major security threats or incidents must be reported to the Emergency Response Officer at BMA's London office without delay. However, this should only be done after the alert has been verified by the CSO.[54]

[54] Bahamas Maritime Authority INFORMATION BULLETIN No. 70 dated 12 April 2007, available at www.bahamasmaritime.com

The notifying party must provide the BMA with the ship's details (name, *official* number, and IMO number), the geographical location of ship, and a description of the cargo if she is laden.[55]

The Bahamas define a major security incident or threat as a hijack, terrorist attack, piracy, any incident involving the use of firearms, any bomb threat, and/or any use or threat of use of force.[56]

China

The IMO database indicates that the recipient of SSAs is the Ministry of Communications of the People's Republic of China (MOC), China Maritime Search and Rescue Center (CNMRCC)[57]

Denmark

Danish procedures call for the SSA to be simultaneously transmitted directly to the Danish Naval Fleet Headquarters[58] and to the shipowners.

Capt. Kjeld Gaard-Frederiksen, Chief of the Danish Navy's Maritime Assistance Service which receives the SSAs from ships, has provided clarifications regarding the management of the SSAs.

The first action taken by the Navy is to contact the CSO to confirm whether or not the SSA is real.

Should a real alert be received, Denmark has established procedures to follow that, whilst confidential, in general would entail the establishment of a cross-agency task force including representatives from the Foreign Ministry, the Department of Defense, the Security and Intelligence Service, the Maritime Administration, as well as others as and when needed.

In all cases the Department of Defense's role is to provide the needed manpower and equipment. The Danish Police are responsible to initiate responsive actions for all incidents within Danish waters or involving ships registered in Denmark. The Foreign Ministry will be involved for all cases involving Danish ships situated outside Danish waters.

Greece

Discussions held in Rostock during a meeting of the BIMCO Maritime Security Committee[59] in May 2007 revealed that the Greek Administration designates the ship

[55] *ibid*
[56] *ibid*
[57] According to the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments. Available via www.imo.org
[58] http://forsvaret.dk/sok/
[59] The BIMCO Maritime Security Committee was established in 1994 to address maritime security issues including drug smuggling, piracy, armed robbery and stowaways. Other issues are addressed including the development and implementation of related regulations and programs. In 2006 the terms

owner as the recipient of SSAs. Concerns at the meeting came up when it was revealed that the steps to take on receipt of an alert were ill-defined at that time. There was an impression that the Administration reportedly did not maintain an around the clock hotline for company security officers to use on receipt of SSAs, but rather had informed owners that the Administration may only be contacted during regular office hours. This understanding raised grave concerns amongst the Committee members with respect to the need to initiate a timely and effective response to SSAs.

However, the IMO database indicates that the recipient of SSAs from Greek ships is the Ministry of Mercantile Marine Joint Rescue Coordination Center, Piraeus (JRCCP), which can be contacted on a 24-hr basis.[60]

Hong Kong, SAR

Information from industry contacts indicate that Hong Kong SAR requires ship security alerts to be received by both the ship owner and the Maritime Administration.

The IMO database indicates that the recipient of SSAs is the Marine Department, The Government of the Hong Kong Special Administrative Region, Marine Rescue Co-ordination Centre (MRCC), Duty Officer.[61] The SSA is to be sent by email[62]

The Hong Kong, SAR MRCC is responsible for coordinating all maritime search and rescue (SAR) missions in international waters of the South China Sea North of Latitude 10 degrees North and West of Longitude 120 degrees East. The Hong Kong MRCC plays a coordinating role for SAR missions involving the Government Flying Service (GFS), Hong Kong Marine Police (Marpol) and/or Fire Services Department (FSD).[63]

Liberia

Information from industry contacts indicate that Liberia requires ship security alerts to be received by both the ship owner and the Administration. This is confirmed and further elaborated upon in the Marine Notice issued by the Republic of Liberia outlining the requirements relating to the ISPS Code.[64]

---

of reference of the committee were expanded to include trade facilitation matters. The author of this working paper chaired the committee from 2005 until 2007. BIMCO, the Baltic and International Maritime Council, is the world's largest non-profit shipping association. See also www.bimco.org

[60] According to the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments. Available via www.imo.org

[61] *ibid*

[62] From guidance on Ship Security Alert Systems available from the Hong Kong SAR Marine Department website http://marsec.mardep.gov.hk/ssa_system.html

[63] From the Hong Kong SAR Marine Department website http://www.mardep.gov.hk/en/home.html

[64] REPUBLIC OF LIBERIA BUREAU OF MARITIME AFFAIRS Marine Notice ISP-001 09/04 TO: ALL SHIPOWNERS, OPERATORS, MASTERS AND OFFICERS OF MERCHANT SHIPS AND AUTHORIZED CLASSIFICATION SOCIETIES. SUBJECT: International Ship & Port Facility Security Code (ISPS Code) available from the website www.liscr.com

After receiving an alert, the CSO shall verify whether the alert is real and then contact the Administration with his findings.
On receipt of the initial alert, the Administration will attempt to contact the CSO, presumably whilst the CSO is seeking to verify whether the SSA is real.

In Liberia the competent authority for managing SSAs is the Office of the Deputy Commissioner for Maritime Affairs c/o the Director of Maritime Security, Liberian International Ship and Corporate Registry.

All the alerts and follow up information are to be sent by e-mail to the Office of the Deputy Commissioner for Maritime Affairs.

The Liberian requirements go a step beyond the SOLAS requirements regarding the information to be contained in SSAs from ships. Whilst the SOLAS requirements call for only three data elements, namely ship's identity, location and an indication that the ship is under threat, the Liberian requirements call for seven elements as well as an optional eighth, being the CSO's name and phone number (if the ship's alert system is capable of providing such information.)

The seven required elements that must be included in alerts issued by Liberian flagged ships are;

1. ship's name,
2. IMO Number,
3. call sign,
4. Maritime Mobile Service Identification (MMSI) number,
5. position,
6. course and speed,
7. date and time (UTC) of the message (alert)

Malta

The IMO database indicates that the recipient of SSAs is the Malta Maritime Authority, Merchant Shipping Directorate.[65] The SSA is to be passed to the Administration from the shipowner.[66]

Marshall Islands

Capt. Thomas F. Heinan, Senior Vice President, Maritime Administration at International Registries, Inc. and Deputy Commissioner of Maritime Affairs for The Republic of the Marshall Islands explains the management of SSAs as follows[67];

Both the Company Security Officer and the Flag State are to receive the initial SSA. On special arrangement and with the knowledge of the Flag State, the Company may arrange for a security contractor to receive the initial SSA as well. In all cases,

[65] According to the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments. Available via www.imo.org
[66] Information received by the author from a Norewgian shipowner's Company Security Officer on 16 November 2007.
[67] Capt. Heinan provided his summary in an email to the author.

however, the Administration must receive the initial SSA.

The Flag State immediately contacts the CSO to confirm the SSA. The Administration will never contact the ship directly, but will rely upon the CSO to confirm the ship's status by whatever means has been devised in accordance with its own security procedures.

Should the SSA be real and it is necessary to mobilize a response, the an Incident Contingency Plan will be initiated that includes contacting the US Department of State Operations Center, the USCG Headquarters Command Center, the IMB, the national authority of the nearest coastal state (if appropriate), and the Marshall Islands Ambassador to Washington, DC. In addition, the Administration immediately initiates hourly long range tracking by satellite through its National Vessel Monitoring System.

Depending on the circumstances, the Administration may avail itself of bilateral and or multilateral arrangements in responding to an SSA. Under the Compact of Free Association between the Marshall Islands and the United States, it has been agreed that US forces will come to the aid of Marshall Islands flagged vessels when called upon to do so.

There is also the Proliferation Security Initiative (PSI) Agreement established between the United States and many countries, including the Marshall Islands. Capt. Heinan feels that the provisions of the PSI Agreement may be called into plan in matters of national security.

Capt. Heinan acknowledges that mobilization in response to an SSA can be very difficult to accomplish with so many varied parties involved. The circumstances surrounding each SSA would dictate how each response would be handled effectively with minimal risk to the safety of the ship and its crew. In order to reduce this confusion, Capt. Heinan feels that the idea of establishing an international coordination mechanism to manage the response to security alerts is an interesting one.

North Korea

The national recipient of SSAs in North Korea is the Maritime Security Division of the Maritime Administration Bureau in Pyangyang.

Although this study was unable to obtain the procedures required by North Korea in respect of the routing of SSAs, the case of the North Korean cargo ship DAI HONG DAN as described in the paper serves well to illustrate how North Korea would initiate action aimed at coming to the aid of a ship faced with a security breach.

Panama

The recipient of ship-to-shore security alerts is the Maritime Security Department at the Panama Maritime Authority, Albrook.[68] The Ship Security Alert (SSA) is to be passed to the Administration from the shipowner.[69]

This is confirmed in a circular issued by the Panama Maritime Authority that designates the shipowner as the competent authority to receive alerts. Upon receipt of an alert, the Company Security Officer (CSO) shall notify the Panama Maritime Authority. The notification shall include the name and the location of the vessel whose SSAS has been activated, in order to inform the relevant Coastal State(s). The communication between the shipowner and the Panama Maritime Authority will be maintained until verification that the situation has returned to normal.[70]

Singapore

For ships registered in Singapore the ship security alert system must transmit the ship-to-shore security alert to the Maritime and Port Authority of Singapore (MPA) Port Master's Office, identifying the ship, its location and indicating that the security of the ship is under threat or has been compromised. The message may be sent using fax or email.[71]

There is no indication that the security alert is to be received by any party other than the MPA, however the regulation does not prohibit this.

Upon receipt of an SSA from a Singaporean ship, the MPA immediately contacts the CSO to verify the security status of the ship. If the ship is within the Singapore Straits the MPA will inform the Singaporean maritime security agencies including the Police, the Coast Guard and the Navy. If the ship is outside Singaporean waters the MPA will contact the respective nearby Coastal States' security forces via the MRCCs. The MPA also reports incidents of piracy and armed robbery to the ReCAAP Information Sharing Center.[72]

St. Kitts & Nevis

Officials at the registry advise that the receipt of SSAs are handled by the St. Kitts & Nevis Director of Maritime Affairs in conjunction with the Ministry responsible for National Security.

---

[68] According to the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments. Available via www.imo.org

[69] Information received by the author from a Norewgian shipowner's Company Security Officer on 16 November 2007.

[70] PANAMA MARITIME AUTHORITY Directorate General of Merchant Marine International Representative Office, N.Y. Merchant Marine Circular No. 133 dated February 2004.

[71] MPA SC No. 11 of 2004 LEGISLATION TO GIVE EFFECT TO THE SPECIAL MEASURES TO ENHANCE MARITIME SECURITY AND ISSUES RELATING THERETO Section 13 Ship Security Alert Systems and the IMO Global Integrated Shipping Information System (GISIS) Maritime Security Database. The information contained in the database is entered by the respective SOLAS Convention Contracting governments. Available via www.imo.org

[72] This information has been provided to the author by the MPA.

St. Kitts & Nevis require that ship security alerts are initially sent to the Company Security Officer or an authorized third party (Security companies such as Securewest have been authorized by the registry to receive security alerts) and by email to the St. Kitts & Nevis Department of Maritime Affairs.

On receipt of an SSA the Company Security Officer or an authorized third party must then verify whether the SSA is genuine. Once that is determined an email must be sent to the Department of Maritime Affairs and to the International Ship Registry to advise them whether or not the SSA is genuine.

In cases where the alert is genuine the following actions are required;

The Company Security officer should e-mail to the Department of Maritime Affairs a copy of the crew list and advise the cargo type(s) and quantity(s) on board and any other relevant information.

The Department of Maritime Affairs will then access the IMO Database to obtain the contact details of the coastal states situated nearby the ship's position. These coastal states will be advised that a security alert has been received from the ship and the given the ship's position. The Director of Maritime Affairs will then liaise with the CSO, the St. Kitts & Nevis Coast Guard and the coastal state(s) for further action.

The Netherlands

For ships registered with the Netherlands, the national requirements stipulate that the SSA must be transmitted directly to the Dutch Coast Guard. However, the option for the transmission to be transmitted via the Company Security Officer is available. Such alerts may only be transmitted to the Coast Guard by telex or fax.[73]

Whilst Dutch Company Security Officers confirm that in practice they are required to inform the Netherlands Coast Guard on receipt of an SSA, they are unsure of what actually will happen after doing so. There have been instances in which the authorities have failed to respond to test SSAs.

Contacts in the Netherlands who have asked to remain anonymous have stated that the Security Group of Koninklijke Vereniging van Nederlandse Reders (KVNR) (the Dutch Shipowners Association) asked representatives from the Dutch Navy how they would react to an SSA. The Navy representative answered that the Navy would dispatch a ship, if there was a Dutch Naval vessel in the proximity of the ship issuing the alert.

Dutch owners would therefore follow the official requirements and then go one or more steps further. By this they have indicated that on receipt of an SSA, Company Security Officers would inform the Coast Guard as required and then seek to engage additional parties including the ship's P and I Club and the ICC/International Maritime Bureau. Such efforts would be made in a proactive approach aimed at expediting an appropriate, timely and effective response.

[73] Consolidated interpretations of Security Rules and Regulations by the Netherlands Shipping Inspectorate (NSI) Version 1.9 dated 26 July 2006

However, if an SSA were to be issued by a ship situated in the English Channel or in US waters, these same owners feel that their hands would be tied, expecting that the local authorities would take complete control of all operations. The owners also harbor concerns that coastal authorities may react by eliminating the threat posed by the 'compromised' ship by "dropping a bomb" on the ship or interfering "in other violent ways," similar to the concerns expressed by seafarers that are addressed later in this paper.

United Kingdom

Information from industry contacts indicates that the UK requires ship security alerts to be received by the ship owner, the Flag State and the Coast Guard at Falmouth.

There are private security companies which have been approved by the British authorities to receive the SSAs on behalf of the shipowners. Securewest International is one of the companies that have received such approval.

The United Kingdom Department for Transport, Transport Security and Contingencies (TRANSEC) Maritime Security Advisor for International Policy has provided the following detailed summary describing the official policy and procedures for handling ship security alerts.

The UK Maritime and Coastguard Agency (MCA)'s Maritime Rescue Co-ordination Centre (MRCC) at Falmouth is the designated authority for the receipt of SSAs from UK flagged ships as well as ships flagged amongst the Red Ensign Group (REG) countries being the Isle of Man, Bermuda, the Cayman Islands and Gibraltar. The SSA message is also sent directly from the ship to the respective Company Security Officer (CSO). SSAs from REG ships are also sent to the relevant Flag State.

On receipt of an SSA, MRCC Falmouth will immediately contact the UK Department for Transport, Transport Security and Contingencies (TRANSEC) Maritime Security Branch and the Metropolitan Police Service (MPS) Counter Terrorist Command (SO15). At this stage the SSA will be unconfirmed. The Company Security Officer (CSO) is responsible for determining whether the alert is genuine or false and then informing the MRCC Falmouth.

In the event that the SSA is confirmed by the CSO to MRCC Falmouth as being genuine, MRCC Falmouth will inform TRANSEC, who will then contact the UK Cabinet Office to advise them of the confirmed SSA.

There are a number of steps that TRANSEC will then take, including;

1. establish if the ship is in UK territorial waters, at a UK port or outside UK territorial waters
2. establish the flag of the ship and contact the UK Joint Terrorism Analysis Centre (JTAC) to request an updated threat assessment of the area in which the ship is located.
3. remain in contact with MRCC Falmouth and the CSO to maintain awareness of all developments.

4. (If the vessel is a cargo ship) contact the Maritime and Coast Guard Agency (MCA) Security Branch for additional information and advice.
5. consult with the Home Office, prior to informing any Port Facilities (if the ship is approaching UK waters. If the ship is in non-UK territorial waters, the Foreign & Commonwealth Office would take the lead.)

Several different agencies may contact TRANSEC seeking information, advice and guidance, including the Police (SO15 – Counter Terrorist Command), the UK Cabinet Office, the Foreign & Commonwealth Office (FCO), the Home Office, the Ministry of Defence, and the MCA.

If the situation develops into a major incident requiring significant TRANSEC/Department for Transport input, a Department for Transport incident room would be established, which would assume responsibility for all external communications with other government departments and agencies and relevant maritime industry contacts. In such situations the Cabinet Office Briefing Room (COBR) may also be formed, liaising with the Department for Transport incident room and the Foreign & Commonwealth Office, in order to ensure that appropriate action is taken.

Genuine SSAs received from the Red Ensign Group (REG) ships flagged to the Isle of Man, Bermuda, Cayman Islands and Gibraltar would be handled as per alerts received from UK flagged ships with only minor differences. On activation of the SSAS on these ships the alert message is sent to the ship's Company Security Officer (CSO) and Flag Administration and MRCC Falmouth. It is then the responsibility of the ship's CSO and/or the Flag State to determine whether the SSA is genuine or false and notify MRCC Falmouth.

If the SSA is genuine, then liaison would be required with both the Flag State and the Governor's/Administrator's office of the relevant Overseas Territory/Crown Dependency. This liaison would be directed by the lead Government Department with advice from the Operations Section of the Maritime Branch. The basic rule of thumb in this instance is to establish liaison with the Governor's office in the first instance and then with the relevant ship registry. If required, the on-call officer would seek advice from a Senior Officer in the Maritime Branch.

As mentioned earlier the United Kingdom allows for private security companies to act as competent authorities on behalf of shipowners. Securewest International is one such company that acts as a competent authority for ships of many registries. Securewest has provided the following description of how they, as a private security company, manage SSAs.

The alert is verified in a secure or covert manner with the vessel. This is done preferably via voice rather than email, and using a secure, easy to remember process.

At the same time the Flag State is notified that an alert has been received and is in the course of being verified. In some cases Flag State’s require almost immediate notification. For example, the US expects contact within 5 minutes of an alert being issued, even though the alert may still be in the course of being verified.

Securewest will also establish voice contact with the CSO or other nominated ship owner contacts.

Once verified, if the alert is false the information is relayed to all parties.

If the alert is real, the Flag State and CSO are notified. Securewest staff will remain engaged as required to continue with any other actions on the instruction of the CSO and/or the Administration. In cases where the ship is being visually tracked, the information can be shared with the Flag State.

United States

The US Coast Guard is the lead US agency regarding merchant ship security, The Coast Guard has considered Ship Security Alert Systems as an important issue in terms of identifying efficient reporting and response procedures.[74]

The procedures are described in a US Coast Guard Commandant's Instruction (COMDTINST) revised on 15 December 2006.[75]

Alerts issued by US-flagged ships are sent directly to the US Coast Guard Commander Pacific Area, US Coast Guard Rescue Coordination Center (RCC) in Alameda, California. For non-US ships, the designated authorities are to advise this same RCC at Almeda when ships in or near US waters have activated their Ship Security Alert Systems. These same non-US designated authorities are also instructed to use the Alameda RCC for all initial requests for assistance in responding to their ships' security alerts.[76]

USCG RCC Alameda is tasked with making the appropriate initial notifications on receipt of ship security alerts. In all such cases, either the CG Operational Commander for the Atlantic Area or the Pacific Area must be notified. These Operational Commanders both have worldwide responsibilities.[77]

On receipt of SSAs from US ships, after notifying the Operational Commander the Alameda RCC will then verify the authenticity of the alert via the ship's Company Security Officer, agent, or local port authority. When the SSA involves a US ship that is outside US territorial waters, the Alameda RCC will, when appropriate, notify the authorities of the Coastal State(s) in the area that the ship is situated.[78]

After the ship security alert has been verified the Alameda RCC will also notify the Commandant Duty Officers at the USCG National Command Center, who will, when needed, initiate follow-on interagency discussions.[79]

---

[74] Advice received by the author from the USCG HQ Office of Vessel Activities, Washington, DC on 2 November 2007
[75] US DHS United States Coast Guard Commandant Instruction 3120.3A "Guidance for Ship Security Alert System (SSAS)" dated 15 December 2006
[76] *ibid*
[77] *ibid*
[78] *ibid*
[79] *ibid*

The procedures are similar for the management of SSAs received from non-US ships that are within US waters. One difference is that the SSA is not verified via the Company Security Officer, as this is the responsibility of the ship's Flag State. Therefore the first step for the Alameda RCC to take is to notify the Commandant Duty Officers at the USCG National Command Center.[80]
Then the Alameda RCC will notify the CG Operational Commander for the Atlantic Area or the Pacific Area depending on the ship's location. Finally the Alameda RCC will contact the Company Security Officer to determine the ship's intentions. Efforts will also be made to obtain details of the known people on board, the ship's itinerary, and any information regarding the situation on the ship. [81]

Whilst the aforementioned steps are outlined in the Coast Guard Commandant's Instructions, one may wonder which agencies would participate in the possible interagency discussions aimed at the evaluation and implementation of the best course of action to take in response to a ship security alert. Owen J. Doherty, Director of the Office of Security at the US Department of Transportation Maritime Administration (MARAD) explains that there are several possibilities regarding which agencies may be involved.

Under the US Maritime Operational Threat Response (MOTR) process, the details of which are classified, several government agencies would come together to decide the appropriate action in a timely manner. The lead may shift from one agency to another during the response. For example, a piracy incident may shift from the Navy to the Department of Justice for appropriate post-event legal action. The MOTR process has been available for about two years.[82]

Liaisons with non-US agencies could also be initiated. Part of the US National Strategy for Maritime Security includes an International Outreach and Coordination Strategy. This part of the National Strategy could help to facilitate multilateral response efforts as it is intended to provide a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and to solicit international support for enhanced maritime security.[83]

Taken together with the International Outreach and Coordination Strategy of the US National Strategy for Maritime Security, the recently released US Coast Guard, Navy and US Marines Cooperative Strategy for 21st Century Seapower[84] could also contribute towards the facilitation of coordinating appropriate SSA response involving non-US agencies.

In response to questions regarding whether the US Cooperative Strategy for 21st Century Seapower could serve to facilitate coordinated rapid responses to ship security alerts, the US Naval Forces Central Command/Combined Maritime Forces Commander Vice Admiral Kevin Cosgriff's staff informed the author that US forces

[80] *ibid*
[81] *ibid*
[82] From information provided to the author by Mr. Owen J. Doherty, Director of the Office of Security at the US Department of Transportation Maritime Administration (MARAD) on 17 November 2007
[83] The US National Strategy for Maritime Security dated 20 September 2005.
[84] Available at the US Navy website http://www.navy.mil/maritime/

and the coalitions in which they participate will always follow the tradition on the high seas which dictates that sailors in distress should be helped. With respect to the Cooperative Strategy for 21st Century Seapower, the Navy sees that as serving as a strategic guide for integrating US maritime forces as well as those of US friends and allies. Although it does not directly address responses to ship security alert systems, the Navy feels that it will shape multilateral agreements which will better manage precious maritime resources and improve command and control, which could, in turn, lead to multi-lateral rapid responses for ships that activate their ship security alert systems.[85]

[85] These clarifications were kindly provided by USN CDR Lynn "Mulan" Chow, Executive Assistant, Commander, US Naval Forces Central Command

IDSS Working Paper Series

1.	Vietnam-China Relations Since The End of The Cold War *Ang Cheng Guan*	(1998)
2.	Multilateral Security Cooperation in the Asia-Pacific Region: Prospects and Possibilities *Desmond Ball*	(1999)
3.	Reordering Asia: "Cooperative Security" or Concert of Powers? *Amitav Acharya*	(1999)
4.	The South China Sea Dispute re-visited *Ang Cheng Guan*	(1999)
5.	Continuity and Change In Malaysian Politics: Assessing the Buildup to the 1999-2000 General Elections *Joseph Liow Chin Yong*	(1999)
6.	'Humanitarian Intervention in Kosovo' as Justified, Executed and Mediated by NATO: Strategic Lessons for Singapore *Kumar Ramakrishna*	(2000)
7.	Taiwan's Future: Mongolia or Tibet? *Chien-peng (C.P.) Chung*	(2001)
8.	Asia-Pacific Diplomac*ies:* Reading Discontinuity in Late-Modern Diplomatic Practice *Tan See Seng*	(2001)
9.	Framing "South Asia": Whose Imagined Region? *Sinderpal Singh*	(2001)
10.	Explaining Indonesia's Relations with Singapore During the New Order Period: The Case of Regime Maintenance and Foreign Policy *Terence Lee Chek Liang*	(2001)
11.	Human Security: Discourse, Statecraft, Emancipation *Tan See Seng*	(2001)
12.	Globalization and its Implications for Southeast Asian Security: A Vietnamese Perspective *Nguyen Phuong Binh*	(2001)
13.	Framework for Autonomy in Southeast Asia's Plural Societies *Miriam Coronel Ferrer*	(2001)
14.	Burma: Protracted Conflict, Governance and Non-Traditional Security Issues *Ananda Rajah*	(2001)
15.	Natural Resources Management and Environmental Security in Southeast Asia: Case Study of Clean Water Supplies in Singapore *Kog Yue Choong*	(2001)
16.	Crisis and Transformation: ASEAN in the New Era *Etel Solingen*	(2001)
17.	Human Security: East Versus West? *Amitav Acharya*	(2001)
18.	Asian Developing Countries and the Next Round of WTO Negotiations *Barry Desker*	(2001)

19. Multilateralism, Neo-liberalism and Security in Asia: The Role of the Asia Pacific Economic Co-operation Forum (2001)
Ian Taylor

20. Humanitarian Intervention and Peacekeeping as Issues for Asia-Pacific Security (2001)
Derek McDougall

21. Comprehensive Security: The South Asian Case (2002)
S.D. Muni

22. The Evolution of China's Maritime Combat Doctrines and Models: 1949-2001 (2002)
You Ji

23. The Concept of Security Before and After September 11 (2002)
a. The Contested Concept of Security
Steve Smith
b. Security and Security Studies After September 11: Some Preliminary Reflections
Amitav Acharya

24. Democratisation In South Korea And Taiwan: The Effect Of Social Division On Inter-Korean and Cross-Strait Relations (2002)
Chien-peng (C.P.) Chung

25. Understanding Financial Globalisation (2002)
Andrew Walter

26. 911, American Praetorian Unilateralism and the Impact on State-Society Relations in Southeast Asia (2002)
Kumar Ramakrishna

27. Great Power Politics in Contemporary East Asia: Negotiating Multipolarity or Hegemony? (2002)
Tan See Seng

28. What Fear Hath Wrought: Missile Hysteria and The Writing of "America" (2002)
Tan See Seng

29. International Responses to Terrorism: The Limits and Possibilities of Legal Control of Terrorism by Regional Arrangement with Particular Reference to ASEAN (2002)
Ong Yen Nee

30. Reconceptualizing the PLA Navy in Post – Mao China: Functions, Warfare, Arms, and Organization (2002)
Nan Li

31. Attempting Developmental Regionalism Through AFTA: The Domestics Politics – Domestic Capital Nexus (2002)
Helen E S Nesadurai

32. 11 September and China: Opportunities, Challenges, and Warfighting (2002)
Nan Li

33. Islam and Society in Southeast Asia after September 11 (2002)
Barry Desker

34. Hegemonic Constraints: The Implications of September 11 For American Power (2002)
Evelyn Goh

35. Not Yet All Aboard…But Already All At Sea Over Container Security Initiative (2002)
Irvin Lim

36. Financial Liberalization and Prudential Regulation in East Asia: Still Perverse? (2002)
Andrew Walter

37. Indonesia and The Washington Consensus (2002)
Premjith Sadasivan

38. The Political Economy of FDI Location: Why Don't Political Checks and Balances and Treaty Constraints Matter? (2002)
Andrew Walter

39. The Securitization of Transnational Crime in ASEAN (2002)
Ralf Emmers

40. Liquidity Support and The Financial Crisis: The Indonesian Experience (2002)
J Soedradjad Djiwandono

41. A UK Perspective on Defence Equipment Acquisition (2003)
David Kirkpatrick

42. Regionalisation of Peace in Asia: Experiences and Prospects of ASEAN, ARF and UN Partnership (2003)
Mely C. Anthony

43. The WTO In 2003: Structural Shifts, State-Of-Play And Prospects For The Doha Round (2003)
Razeen Sally

44. Seeking Security In The Dragon's Shadow: China and Southeast Asia In The Emerging Asian Order (2003)
Amitav Acharya

45. Deconstructing Political Islam In Malaysia: UMNO'S Response To PAS' Religio-Political Dialectic (2003)
Joseph Liow

46. The War On Terror And The Future of Indonesian Democracy (2003)
Tatik S. Hafidz

47. Examining The Role of Foreign Assistance in Security Sector Reforms: The Indonesian Case (2003)
Eduardo Lachica

48. Sovereignty and The Politics of Identity in International Relations (2003)
Adrian Kuah

49. Deconstructing Jihad; Southeast Asia Contexts (2003)
Patricia Martinez

50. The Correlates of Nationalism in Beijing Public Opinion (2003)
Alastair Iain Johnston

51. In Search of Suitable Positions' in the Asia Pacific: Negotiating the US-China Relationship and Regional Security (2003)
Evelyn Goh

52. American Unilaterism, Foreign Economic Policy and the 'Securitisation' of Globalisation (2003)
Richard Higgott

53. Fireball on the Water: Naval Force Protection-Projection, Coast Guarding, Customs Border Security & Multilateral Cooperation in Rolling Back the Global Waves of Terror from the Sea (2003)
Irvin Lim

54. Revisiting Responses To Power Preponderance: Going Beyond The Balancing-Bandwagoning Dichotomy (2003)
Chong Ja Ian

55. Pre-emption and Prevention: An Ethical and Legal Critique of the Bush Doctrine and Anticipatory Use of Force In Defence of the State (2003)
Malcolm Brailey

56. The Indo-Chinese Enlargement of ASEAN: Implications for Regional Economic Integration (2003)
Helen E S Nesadurai

57. The Advent of a New Way of War: Theory and Practice of Effects Based Operation (2003)
Joshua Ho

58. Critical Mass: Weighing in on Force Transformation & Speed Kills Post-Operation Iraqi Freedom (2004)
Irvin Lim

59. Force Modernisation Trends in Southeast Asia (2004)
Andrew Tan

60. Testing Alternative Responses to Power Preponderance: Buffering, Binding, Bonding and Beleaguering in the Real World (2004)
Chong Ja Ian

61. Outlook on the Indonesian Parliamentary Election 2004 (2004)
Irman G. Lanti

62. Globalization and Non-Traditional Security Issues: A Study of Human and Drug Trafficking in East Asia (2004)
Ralf Emmers

63. Outlook for Malaysia's 11th General Election (2004)
Joseph Liow

64. Not *Many* Jobs Take a Whole Army: Special Operations Forces and The Revolution in Military Affairs. (2004)
Malcolm Brailey

65. Technological Globalisation and Regional Security in East Asia (2004)
J.D. Kenneth Boutin

66. UAVs/UCAVS – Missions, Challenges, and Strategic Implications for Small and Medium Powers (2004)
Manjeet Singh Pardesi

67. Singapore's Reaction to Rising China: Deep Engagement and Strategic Adjustment (2004)
Evelyn Goh

68. The Shifting Of Maritime Power And The Implications For Maritime Security In East Asia (2004)
Joshua Ho

69. China In The Mekong River Basin: The Regional Security Implications of Resource Development On The Lancang Jiang (2004)
Evelyn Goh

70. Examining the Defence Industrialization-Economic Growth Relationship: The Case of Singapore (2004)
Adrian Kuah and Bernard Loo

71. "Constructing" The Jemaah Islamiyah Terrorist: A Preliminary Inquiry (2004)
Kumar Ramakrishna

72. Malaysia and The United States: Rejecting Dominance, Embracing Engagement (2004)
Helen E S Nesadurai

73. The Indonesian Military as a Professional Organization: Criteria and Ramifications for Reform (2005)
John Bradford

74. Martime Terrorism in Southeast Asia: A Risk Assessment (2005)
Catherine Zara Raymond

75. Southeast Asian Maritime Security In The Age Of Terror: Threats, Opportunity, And Charting The Course Forward (2005)
John Bradford

76. Deducing India's Grand Strategy of Regional Hegemony from Historical and Conceptual Perspectives (2005)
Manjeet Singh Pardesi

77. Towards Better Peace Processes: A Comparative Study of Attempts to Broker Peace with MNLF and GAM (2005)
S P Harish

78. Multilateralism, Sovereignty and Normative Change in World Politics (2005)
Amitav Acharya

79. The State and Religious Institutions in Muslim Societies (2005)
Riaz Hassan

80. On Being Religious: Patterns of Religious Commitment in Muslim Societies (2005)
Riaz Hassan

81. The Security of Regional Sea Lanes (2005)
Joshua Ho

82. Civil-Military Relationship and Reform in the Defence Industry (2005)
Arthur S Ding

83. How Bargaining Alters Outcomes: Bilateral Trade Negotiations and Bargaining Strategies (2005)
Deborah Elms

84. Great Powers and Southeast Asian Regional Security Strategies: Omni-enmeshment, Balancing and Hierarchical Order (2005)
Evelyn Goh

85. Global Jihad, Sectarianism and The Madrassahs in Pakistan (2005)
Ali Riaz

86. Autobiography, Politics and Ideology in Sayyid Qutb's Reading of the Qur'an (2005)
Umej Bhatia

87. Maritime Disputes in the South China Sea: Strategic and Diplomatic Status Quo (2005)
Ralf Emmers

88. China's Political Commissars and Commanders: Trends & Dynamics (2005)
Srikanth Kondapalli

89. Piracy in Southeast Asia New Trends, Issues and Responses (2005)
Catherine Zara Raymond

90. Geopolitics, Grand Strategy and the Bush Doctrine (2005)
Simon Dalby

91. Local Elections and Democracy in Indonesia: The Case of the Riau Archipelago (2005)
Nankyung Choi

92. The Impact of RMA on Conventional Deterrence: A Theoretical Analysis (2005)
Manjeet Singh Pardesi

93 Africa and the Challenge of Globalisation (2005)
Jeffrey Herbst

94 The East Asian Experience: The Poverty of 'Picking Winners (2005)
Barry Desker and Deborah Elms

95 Bandung And The Political Economy Of North-South Relations: Sowing The Seeds For Revisioning International Society (2005)
Helen E S Nesadurai

96 Re-conceptualising the Military-Industrial Complex: A General Systems Theory Approach (2005)
Adrian Kuah

97 Food Security and the Threat From Within: Rice Policy Reforms in the Philippines (2006)
Bruce Tolentino

98 Non-Traditional Security Issues: Securitisation of Transnational Crime in Asia (2006)
James Laki

99 Securitizing/Desecuritizing the Filipinos' 'Outward Migration Issue'in the Philippines' Relations with Other Asian Governments (2006)
José N. Franco, Jr.

100 Securitization Of Illegal Migration of Bangladeshis To India (2006)
Josy Joseph

101 Environmental Management and Conflict in Southeast Asia – Land Reclamation and its Political Impact (2006)
Kog Yue-Choong

102 Securitizing border-crossing: The case of marginalized stateless minorities in the Thai-Burma Borderlands (2006)
Mika Toyota

103 The Incidence of Corruption in India: Is the Neglect of Governance Endangering Human Security in South Asia? (2006)
Shabnam Mallick and Rajarshi Sen

104 The LTTE's Online Network and its Implications for Regional Security (2006)
Shyam Tekwani

105 The Korean War June-October 1950: Inchon and Stalin In The "Trigger Vs Justification" Debate (2006)
Tan Kwoh Jack

106	International Regime Building in Southeast Asia: ASEAN Cooperation against the Illicit Trafficking and Abuse of Drugs *Ralf Emmers*	(2006)
107	Changing Conflict Identities: The case of the Southern Thailand Discord *S P Harish*	(2006)
108	Myanmar and the Argument for Engagement: *A Clash of Contending Moralities?* *Christopher B Roberts*	(2006)
109	TEMPORAL DOMINANCE Military Transformation and the Time Dimension of Strategy *Edwin Seah*	(2006)
110	Globalization and Military-Industrial Transformation in South Asia: An Historical Perspective *Emrys Chew*	(2006)
111	UNCLOS and its Limitations as the Foundation for a Regional Maritime Security Regime *Sam Bateman*	(2006)
112	Freedom and Control Networks in Military Environments *Paul T Mitchell*	(2006)
113	Rewriting Indonesian History The Future in Indonesia's Past *Kwa Chong Guan*	(2006)
114	Twelver Shi'ite Islam: Conceptual and Practical Aspects *Christoph Marcinkowski*	(2006)
115	Islam, State and Modernity : Muslim Political Discourse in Late 19th and Early 20th century India *Iqbal Singh Sevea*	(2006)
116	'*Voice of the Malayan Revolution*': The Communist Party of Malaya's Struggle for Hearts and Minds in the 'Second Malayan Emergency' (1969-1975) *Ong Wei Chong*	(2006)
117	"From Counter-Society to Counter-State: Jemaah Islamiyah According to PUPJI" *Elena Pavlova*	(2006)
118	The Terrorist Threat to Singapore's Land Transportation Infrastructure: A Preliminary Enquiry *Adam Dolnik*	(2006)
119	The Many Faces of Political Islam *Mohammed Ayoob*	(2006)
120	Facets of Shi'ite Islam in Contemporary Southeast Asia (I): Thailand and Indonesia *Christoph Marcinkowski*	(2006)
121	Facets of Shi'ite Islam in Contemporary Southeast Asia (II): Malaysia and Singapore *Christoph Marcinkowski*	(2006)
122	Towards a History of Malaysian Ulama *Mohamed Nawab*	(2007)
123	Islam and Violence in Malaysia *Ahmad Fauzi Abdul Hamid*	(2007)

124	Between Greater Iran and Shi'ite Crescent: Some Thoughts on the Nature of Iran's Ambitions in the Middle East *Christoph Marcinkowski*	(2007)
125	Thinking Ahead: Shi'ite Islam in Iraq and its Seminaries (hawzah 'ilmiyyah) *Christoph Marcinkowski*	(2007)
126	The China Syndrome: Chinese Military Modernization and the Rearming of Southeast Asia *Richard A. Bitzinger*	(2007)
127	Contested Capitalism: Financial Politics and Implications for China *Richard Carney*	(2007)
128	Sentinels of Afghan Democracy: The Afghan National Army *Samuel Chan*	(2007)
129	The De-escalation of the Spratly Dispute in Sino-Southeast Asian Relations *Ralf Emmers*	(2007)
130	War, Peace or Neutrality:An Overview of Islamic Polity's Basis of Inter-State Relations *Muhammad Haniff Hassan*	(2007)
131	Mission Not So Impossible: The AMM and the Transition from Conflict to Peace in Aceh, 2005–2006 *Kirsten E. Schulze*	(2007)
132	Comprehensive Security and Resilience in Southeast Asia: ASEAN's Approach to Terrorism and Sea Piracy *Ralf Emmers*	(2007)
133	The Ulama in Pakistani Politics *Mohamed Nawab*	(2007)
134	China's Proactive Engagement in Asia: Economics, Politics and Interactions *Li Mingjiang*	(2007)
135	The PLA's Role in China's Regional Security Strategy *Qi Dapeng*	(2007)
136	War As They Knew It: Revolutionary War and Counterinsurgency in Southeast Asia *Ong Wei Chong*	(2007)
137	Indonesia's Direct Local Elections: Background and Institutional Framework *Nankyung Choi*	(2007)
138	Contextualizing Political Islam for Minority Muslims *Muhammad Haniff bin Hassan*	(2007)
139	Ngruki Revisited: Modernity and Its Discontents at the Pondok Pesantren al-Mukmin of Ngruki, Surakarta *Farish A. Noor*	(2007)
140	Globalization: Implications of and for the Modern / Post-modern Navies of the Asia Pacific *Geoffrey Till*	(2007)
141	Comprehensive Maritime Domain Awareness: An Idea Whose Time Has Come? *Irvin Lim Fang Jau*	(2007)
142	Sulawesi: Aspirations of Local Muslims *Rohaiza Ahmad Asi*	(2007)

143 Islamic Militancy, Sharia, and Democratic Consolidation in Post-Suharto Indonesia (2007)
Noorhaidi Hasan

144 Crouching Tiger, Hidden Dragon: The Indian Ocean and The Maritime Balance of Power in Historical Perspective (2007)
Emrys Chew

145 New Security Dimensions in the Asia Pacific (2007)
Barry Desker

146 Japan's Economic Diplomacy towards East Asia: Fragmented Realism and Naïve Liberalism (2007)
Hidetaka Yoshimatsu

147 U.S. Primacy, Eurasia's New Strategic Landscape,and the Emerging Asian Order (2007)
Alexander L. Vuving

148 The Asian Financial Crisis and ASEAN's Concept of Security (2008)
Yongwook RYU

149 Security in the South China Sea: China's Balancing Act and New Regional Dynamics (2008)
Li Mingjiang

150 The Defence Industry in the Post-Transformational World: Implications for the United States and Singapore (2008)
Richard A Bitzinger

151 The Islamic Opposition in Malaysia:New Trajectories and Directions (2008)
Mohamed Fauz Abdul Hamid

152 Thinking the Unthinkable: The Modernization and Reform of Islamic Higher Education in Indonesia (2008)
Farish A Noor

153 Outlook for Malaysia's 12th General Elections (2008)
Mohamed Nawab Mohamed Osman, Shahirah Mahmood and Joseph Chinyong Liow

154 The use of SOLAS Ship Security Alert Systems (2008)
Thomas Timlen