

# Potential consequences of imprecise security assessments

J.U. Schröder<sup>1</sup>, M.Q. Mejia Jr.<sup>1</sup>, P.K. Mukherjee<sup>1</sup>, F.M. Manolis<sup>1</sup>, S. Dreeßen<sup>2</sup>

<sup>1</sup>World Maritime University, Malmö, Sweden

<sup>2</sup>Scandlines, Rostock, Germany

## Abstract

The recently implemented International Shipboard and Port Facility Security (ISPS) Code [1] requires security assessments for ships and port facilities. Although Part B provides elaborate guidance on issues to be observed and included into such risk assessments a generally accepted methodology to carry out such risk assessments is not prescribed in the Code. This allows for subjective expert judgement as the basis for security risk assessments. However, subjective risk assessment will vary in scope and results. This is a normal feature of any risk assessment involving opinions of different individuals. This would in principle not cause any harm if legal consequences would not be involved in case a ship or its cargo was subject to a security incident. Legal experts voiced opinions that in such a situation they would challenge the security risk assessment. In case that issues connected to the security incident in question that harmed ship or cargo was not addressed properly in the security assessment they would question the seaworthiness of the ship. This would of course have far reaching liability consequences for ship owners. The question therefore is how ship owners can be protected against uncertainty resulting from imprecise standards for security risk assessment of the ISPS Code.

*Keywords:* Maritime security, security risk assessment, seaworthiness

## 1 Introduction

The ISPS Code [1] requires in its Part A Sec. 8 a shipboard security risk assessment to be carried out as “an essential and integral part of the process of developing and updating the ship security plan.” Guidance is given in the non-

mandatory Part B of the Code in the corresponding Para. 8. A comprehensive list of issues to be considered when such a security risk assessment is carried is provided in this regulation. Apart from this non-binding list of issues no methodology is suggested. Only brief and general advice is given in paragraph 8.2, where the Company Security Officer (CSO) is referred to “any specific guidance offered by the Contracting Governments”. To the knowledge of the authors only one country, the United States, has specified such guidance [2]. This leaves it up to the CSO to define a suitable methodology. Principally there is nothing wrong with such an approach. In fact it is used widely throughout various approaches to the assessment of safety and security related matters. One aspect of concern is, however, that such an approach involves a certain degree of deviation and comparability of the results provided by different risk assessment teams. The resulting question could therefore be why to discuss this issue any further.

The answer to this is relatively simple. The security risk assessment forms the basis of the ship security plan, which creates the security system on board a ship. A plan not addressing all relevant maritime security areas of concern could therefore be considered as not sufficient and subsequently open up the opportunity to challenge the seaworthiness of the ship in question. This would clearly result in far reaching liability issues for the ship owner. Although no case is yet known in the above-mentioned security context, attempts have been undertaken to challenge the seaworthiness in court with respect to the International Safety Management (ISM) Code [3], a Code bearing many similarities to the ISPS Code. Prominent examples were *Eurasian Dream*, *Torepo*, and *Patraikos II* [4]. The question therefore remains if a cargo owner could challenge a ship owner for lacking due diligence with respect to the scope of a security risk assessment if this risk assessment has not addressed areas of concern which led to cargo damage in a security incident. If this is the case would it not be desirable to have stricter guidelines for ship security risk assessment, which would limit the liability of ship owners?

This paper is intended to investigate the issues mentioned above and to highlight potential consequences. It will furthermore outline a framework intended to safeguard sufficient security risk assessment and discuss advantages and disadvantages linked to minimum standards for security risk assessment.

## **2 What can ship crews do against maritime security threats?**

The options available to ship’s crews when dealing with maritime security threats are very limited. To begin with, ship crews are neither trained nor attuned to responding to security threats. Seafarers are only beginning today to train, as a result of ISPS Code implementation, to deter and prevent threats and to mitigate the effects of security incidents. Nevertheless, their security tasks are only collateral to their primary functions as navigators and engineers. They cannot be expected to react to a security threat in the same manner as security professionals who are trained to detect, intercept, delay, or neutralize targets [5]. Indeed, the proposed security-related amendments to the International Convention on

Standards of Training, Certification and Watchkeeping for Seafarers (STCW) concentrate on the integration of ship security officer (SSO) training within the curriculum and not combat or weapons training [6]. This complements the long-standing policy of various maritime organizations against the arming of seafarers in spite of rapidly rising levels of maritime violence in the past two decades.

Prevailing manning levels and the demanding nature of shipboard life are also factors that limit the options available to ship crews in dealing with security threats. Crews have simply become “too small and too busy to offer any sort of realistic protection against a human intelligence actively seeking to subvert the ship to its wicked purpose” [7].

The most prevalent security threats facing ships today are piracy and armed robbery. The groups that commit these unlawful acts come in different levels of organization and sophistication and employ varieties of *modi operandi*. One variety that is popular in the waters of Malacca Straits and Indonesia is one where a rubber boat carrying the attackers would come alongside the merchant vessel, climb on board using grappling hooks, bind the crew with rope, collect all personal valuables, and raid the ship’s safe. Many attacks result in some sort of injury to the crew. In a few attacks where the vessel and its entire cargo were hijacked, crew members have been killed or seriously injured either as a direct result of violence from the attackers or while trying to flee or escape. According to statistics collected by the International Chamber of Commerce-International Maritime Bureau (ICC-IMB) for the year 2004, a total of 325 attacks were reported by ships, of which 197 involved pirates and armed robbers who were armed with guns, knives, or other weapons. During this period, 234 persons were either kidnapped or taken hostage, 59 were injured, 30 were killed, and 30 are still missing. 226 ships were boarded, 12 ships were fired upon, and 11 ships were hijacked [8].

The threat of maritime terrorism, on the other hand, remains largely a potential one. Compared to piracy and armed robbery against ships, there are relatively fewer incidents of maritime terrorism. The *Santa Maria* (1961), *Achille Lauro* (1985), *City of Poros* (1988), *Our Lady of Mediatrix* (2000), *USS Cole* (2000), *Limburg* (2002), *Superferry 14* (2004), and *Doña Ramona* (2005) are some of the few that readily come to mind. Also, a security threat involving terrorism carries with it a potential for much greater damage and injury. While pirates and armed robbers aim to escape with their lives and the stolen items, terrorists do not seek the cargo or personal valuables. Terrorists are highly trained in the use of violence and stand ready, if need be, to kill others or to give up their own lives [9].

There are other threats to the security of ship’s crews aside from piracy, armed robbery, and terrorism. One threat for which the ISPS Code was also developed is the problem of stowaways. According to IMO statistics, 265 cases were reported in 2002 and 185 in 2003 [10]. The discovery of stowaways is a serious violation of the integrity and security of the vessel, and stowaways who find themselves in desperate situations could resort to violence against the crew. By the same token, there have been incidents [11] where stowaways have been abused and even killed by the crew.

It is too early to determine what specific effect the ISPS Code has had in terms of the risk profile of ships. One can only assume that the conscientious implementation of the Code would increase deterrence against criminal attacks and therefore result in a lower risk profile. It is now more than a year after the Code entered into force and a number of organizations have issued positive comments on the shipping industry's compliance. The United States Coast Guard (USCG) praised the international maritime community for having "demonstrated a significant level of compliance with the ISPS Code on the July 1st (2004) implementation date" [12, p.2]. The USCG also reported a continuing downward trend in the overall rate of ISPS-related major control actions (MCA), that is, denial of entry into port, expulsion from port, and ship detention. In July 2004, the rate was 2.5%. By yearend, the MCA rate had dropped to 1.5% or 92 out of 6,087 inspections [12, pp.6, 25]. Similar praise was given by the secretariats of both the Paris and Tokyo Memoranda of Understanding on Port State Control. The Paris MoU reported a 1.46% ISPS-related detention rate [13] while the Tokyo MoU reported 1% [14]. However, even in the face of such positive comments it is important to note that the question of whether significant ISPS compliance – as determined during port state control – translates to more secure ships and seafarers, is a complicated one.

After the passage of time and the accumulation of sufficient data, it might eventually be feasible to measure the level of success of the Code. As regards the threats of piracy and armed robbery, IMB statistics show a decrease in the number of attacks reported between the years 2003 (445 attacks) and 2004 (325 attacks) [8, p.6]. They also show a significant decrease in the number of attacks according to type of attack (attempted boarding, detention, firing, hijack, robbery, etc.), type of violence employed (hostage-taking/kidnapping, assault, injury, killing), and type of arms used (guns, knives, other weapons) for the first quarter of 2005 compared to the same period of the previous five years [15]. It would be interesting to see whether in a few years this turns out to be the beginning of a discernable decrease in reported incidents. As far as the threat of terrorism is concerned, the lack of critical mass in statistical data will prove the task of determining success to be even more challenging.

To measure the ISPS Code's success would be to determine whether ship crews are able to achieve the Code's objectives of effectively deterring and preventing unlawful acts and mitigating the consequences of an actual security incident. As mentioned earlier, ship crews are already at a disadvantage because of low manning levels and heavy workloads. Also, attention to security is not innate in the seafarer in the same way that safety has come to be. In addition, because an offensive capability is inconsistent with the objectives of the ISPS Code, the only "weapons" available to ship's crew are safety equipment such as fire hoses and signal flares. In other words, the answer to the question *Can ship crews effectively react to security incidents?* is a qualified "yes," that is, to the extent that training and proficiency in deterrence and other security tasks are required by the ISPS Code. Once deterrence and prevention have failed and a security incident is imminent or underway, the actions available to the crew are basically limited to activating the ship security alarm system (SSAS), calling emergency

stations, evacuating the ship, and acting on instructions from the contracting government.

There is not much a ship's crew can do once an armed robber or terrorist has decided to strike in spite of the ship's ISPS-compliant security system. Merchant ships are not equipped with either an active defence or offence capability. In fact as the *USS Cole* incident so clearly demonstrated, even a technologically advanced guided missile destroyer manned by professional naval warriors could be limited in its response options once the watercraft, its lethal cargo, and its crew of suicide bombers have already blown up in a thousand pieces. In the case of merchant vessels, security risk management (in many cases, risk avoidance) through the ISPS Code is offered as the optimum solution.

### **3 Liability for Unseaworthiness in the Context of Maritime Security**

The central issue here is whether non-compliance with the ISPS Code constitutes a failure of seaworthiness which in turn can lead to potential liability on the part of the carrier or shipowner. An affirmative conclusion may arguably be attributed to a dubious ship security plan based on deficient or inadequate risk assessment. The problem, of course, is that there are neither any decided cases on this point in relation to the ISPS Code, nor is there any authoritative or scholarly legal literature. (See however, [16, p. 370] where the authors refer to deficiency in ISPS compliance, in particular, lack of crew security training, deficient ISPS documentation and master or crew negligence as possibly constituting unseaworthiness.) At best an analogy can be drawn with liability implications for failure of seaworthiness in relation to the ISM Code in the context of which some views have been expressed and some tangential references have been made judicially. These will be examined in the following text.

#### **3.1 What is seaworthiness?**

For the discussion to be meaningful, it must obviously begin with a review of what is the legal concept of seaworthiness. This is a notion peculiar to maritime law and exists mainly within the domain of commercial maritime law; to be precise, in contracts of carriage under bills of lading, in charterparties and in marine insurance contracts tempered by relevant statutory provisions. Judicially, a seaworthy ship has been described as one that is "...in a fit state as to repairs, equipment, crew and in all other respects, to encounter the ordinary perils of the sea of the voyage" (*Dixon v. Sadler* [17]). A question that arises is whether a security risk is an ordinary peril. Another judicial definition describes a seaworthy ship as "...one which is reasonably fit for its intended purpose" (*Phipps v. ss Santa Maria* [18]). If without ISPS Code certification a vessel cannot be insured or utilised to transport cargo internationally, can it be argued that it is not "fit for its intended purpose" [19, p. 1601]? The classic definition of "seaworthiness" in the case of *F.C. Bradley & Sons Ltd. v. Federal Steam Navigation Co.* [20, p. 454] where approving a statement on *Carver on Carriage*

by *Sae* the court held that “[T]he ship must have that degree of fitness which an ordinary careful owner would require his vessel to have at the commencement of her voyage having regard to all probable circumstances of it.”

“Seaworthiness is not an absolute concept; it is relative to the nature of the ship, to the particular voyage or even to the particular stage of the voyage on which the ship is engaged.” ([21] p. 315, approved by [22] at p. 197. See [23] para. 126).

### **3.2 Seaworthiness in Carriage Law: Application of Hague-Visby Rules**

Article III, Rule 1 requires a carrier to exercise due diligence before and at the beginning of the voyage to make the ship seaworthy and cargoworthy. The duty pertains to “all reasonably foreseeable eventualities” but in “normal circumstances”. [24, p. 19.] This raises the question of whether a security incident is a reasonably foreseeable eventuality in normal circumstances. In legal terms the test is an objective one, no doubt, but its application may be fraught with confusion.

In *The Eurasian Dream* [23, para. 123] decision, the court identified the following steps in terms of the application of the Hague-Visby Rules:

First, the claimant must carry the burden of proving unseaworthiness. Second, the claimant must prove causation, i.e., that the loss or damage was proximately caused by unseaworthiness (See [19], p. 8 for what constitutes “proximate cause”). Third, the defendant must carry burden of proof to invoke the defence of due diligence; [25, p. 5]. Fourth, if the defendant fails to discharge the burden, he would not be entitled to rely on any of the Art. IV, r. 2 exceptions.

This brings us to the fundamental question of whether a failure to comply with the ISPS Code per se is a breach of the requirement to exercise due diligence to make a ship seaworthy. In *The Eurasian Dream* the failure to have adequate documentation (Fire Manual in) may have been a consideration in the mind of the court. Support in the affirmative for this proposition is doubtful given the paucity of authority. A better proposition is that compliance with the ISPS Code is indicative of due diligence exercised by the defendant [19, p. 1601].

It is perhaps a fair conclusion that compliance with the ISPS Code on balance has better evidentiary use as defence of due diligence than non-compliance as a positive indicator of unseaworthiness in respect of Hague-Visby Rules (For the same conclusion in respect of the ISM Code, see [26] pp. 11-12.) At any rate, a judicial pronouncement on liability arising out of unseaworthiness, whether it is in the affirmative or in the negative, will surely impact, or at least raise some serious questions relating to security risk assessment.

## **4 Maritime security assessment as a risk control option for the protection of the ship owner**

Following the discussions of the earlier sections of this paper it can be concluded that ship crews can prevent or mitigate security incidents only to a certain extent. Security incidents can result from a number of sources and involve a wide range

of methodologies. It is therefore very difficult to consider all potential security threats appropriately. At the same time ship owners would benefit from a stricter definition of the scope of maritime security assessments, as they cannot foresee all potential sources of such incidents. The question to be raised is how this can be achieved taking all the aforementioned aspects into consideration.

The ISPS Code [1] apart from its Sec. 8 in parts A and B does not provide any more specific guidance on how to carry out shipboard security risk assessments. Part A (refer in particular to 8.4) refers to the identification of existing security measures, the evaluation of key shipboard operations to be protected, the identification of threats to these operations and the identification of weaknesses resulting from infrastructure, policies, etc. Part B is more elaborate and provides a number of issues to be considered in shipboard security risk assessments (refer to Part B Sec. 8.7 – 8.10). Although this list is not very long it is specific guidance for risk assessments. The only problem involved is that Part B is not mandatory. One could of course say that in the absence of other guidelines one has to observe the issues mentioned in Part B. However, not all maritime stakeholders are of this opinion. Recognized organizations (RO's) provide different guidelines for shipboard security risk assessments. A majority, such as the American Bureau of Shipping (ABS) or Lloyd's Register favours the risk assessment guidelines provided by the United States Coast Guard (USCG) [2]. The USCG guidelines, however, do not specifically relate to the ISPS Code. They have been developed for security risk assessments in general and are lacking therefore specific cross-references to the relevant ISPS Code requirements. Two RO's, Det Norske Veritas (DNV) [27] and Germanischer Lloyd (GL) [28], have developed guidelines based on checklists which have a very close relationship to the ISPS Code. Both approaches apart from varying methodologies have another significant difference. The USCG guidelines do not include any statements about likelihoods of security threats, whereas the DNV-GL approach allows for a consideration of likely threats only. This means that on the one hand shipowners who follow the USCG approach strictly have to document any potential security threat and develop mitigation strategies of those issues which can result in severe consequences. If one would follow this approach one has to provide for a number of costly measures. On the other hand shipowners following the DNV-GL approach have to update their security assessments frequently depending on the latest security information available. Potential disputes about the validity and appropriateness of the security information are not likely to be avoided. To make it even more confusing the USCG requires all ships calling US ports to comply with both parts of the ISPS Code – A and B. The result therefore will to a certain degree most likely be frustration by a shipowner who is confronted with the task of arranging for security risk assessments on board his ships. What could therefore be suggestions to overcome this problem?

## 5 Conclusions and summary

Any suggestions regarding solutions for the above-mentioned problems have to consider the following three issues:

- Ship crews have limited capabilities to mitigate security attacks against their ships.
- Motives/reasons for security incidents result from a large variety of sources.
- Shipowners need certainty about scope and applicable requirements for the shipboard security as far as their liability is concerned.

In this respect it is remarkable to see that a number of IMO instruments or documents issued within the IMO framework focussing on risk assessment in general or maritime security in a wider sense have taken some of the above mentioned points into consideration. They provide for more guidelines on the contents of risk assessment on their area of interest.

One example, to be mentioned in this context, is the guideline on Formal Safety Assessment (FSA) [29]. The 2002 extended guidelines include not only “technical” risk assessment, but also human reliability assessment with detailed descriptions of methodologies. Another example is the guideline on places of refuge [30]. In order to assist maritime administrations the IMO provided for these guidelines where in section 3 a dedicated part deals with risk assessment only. Although no specific methodologies are described at least a number of issues to be considered during the risk assessment is listed. It is hoped that the place of refuge guidelines will be extended and updated similar to the FSA guidelines.

Most recently another remarkable example was given through the IMO/ILO Code of Practice on Security in Ports [31]. These guidelines provide for a much more defined framework for a number of issues around port security. The risk assessment part was given special attention in this code. A full methodology is suggested here. This goes significantly beyond the ISPS Code requirements. This example is not the only one. The European Commission (EC) recently suggested a directive on enhancing port security [32]. Annex I deals with the port security assessment. Although the specifications made there do not go beyond the ISPS requirements it is at least remarkable that the EC found it necessary to address this subject.

The question still remains why is special attention only paid to port security and not to ship security as well? Although ships are the weaker link in the security chain they still have an important part to play in the security framework. The lack of more specific guidelines disadvantages shipowners. Therefore more detailed guidelines should be designed for ships security assessments. These guidelines should address the following points:

- List of security incidents that ship crews can respond to depending on:
  - Type of the ship,
  - Type of the cargo,
  - Size of the crew,
  - Trading area.

- List of key shipboard operations (incl. safety measures) which have to be protected
- List of restricted areas where special security measures should be introduced

The above listed issues are just only a very general outline of key issues to be observed in more detailed guidelines. These guidelines would be in line with current developments on other maritime security related issues, i.e. port security. More communication of the different stakeholders in politics, shipping and research is needed to develop and implement such elaborate guidelines in shipping.

## Disclaimer

The views expressed in this paper are the personal views of the authors and not necessarily those of the employers of the authors.

## References

- [1] International Ship and Port Facility Security Code; IMO Doc. SOLAS/CONF.5/34, 17 December 2002.
- [2] NVIC. 10-02, Security Guidelines for Vessels; United States Coast Guard, 21 October 2002. <http://www.uscg.mil/hq/g-m/nvic/02/10-02.pdf>
- [3] International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code); IMO Doc. A. 18/Res. 741, 17 November 1993.
- [4] North of England P&I Club, The Exercise of Due Diligence in Employing Crew. *Signals – the Loss Prevention Newsletter for North of England Members*, Issue 50, p. 6, January 2003. <http://195.173.17.24/risk/publications/newsletters/pdf/signals50.pdf>
- [5] Emerson, S.D. & Nadeau, J., A Coastal Perspective on Security. *Journal of Hazardous Materials*, 104, p. 4, 2003.
- [6] Measures to Enhance Maritime Security, Training and Certification Requirements for Company and Port Facility Security Officers, Report of the Working Group; IMO Doc. STW 36/WP. 2, 12 January 2005.
- [7] Insight and Opinion; Lloyd's List, 7 May 2003.
- [8] International Maritime Bureau, *Piracy and Armed Robbery against Ships: Annual Report 1 January-31 December 2004*, ICC-IMB: Essex, 2005.
- [9] Mejia, M., Maritime Gerrymandering: Dilemmas in Defining Piracy, Terrorism, and other Acts of maritime Violence. *Journal of International Commercial Law*, 2(2), p. 165, 2003.
- [10] Reports on Stowaway Incidents: Annual Statistics for the Years 2002 and 2003; IMO Doc. FAL. 2/Circ. 83, p. 11, 12 July 2004.
- [11] Eales, B., Getting away with Murder? *Fairplay*, pp. 16-18, 18 November 2004; also Moore, A., Crime on the high Seas. *Fairplay*, pp. 18-19, 18 November 2004.

- [12] United States Coast Guard (USCG), *Port State Control in the United States: annual report 2004*, USCG: Washington, 2005.
- [13] The Paris Memorandum of Understanding on Port State Control, *Annual Report 2004: Changing Course*, Paris MoU on PSC: Rotterdam, p. 46, 2005.
- [14] Memorandum of Understanding on Port State Control in the Asia-Pacific Region, *Annual Report on Port State Control in the Asia-Pacific Region 2004*, Tokyo MoU on PSC: Tokyo, p. 3, 2005.
- [15] International Maritime Bureau, *Piracy and Armed Robbery against Ships: Report for the Period 1 January-31 March 2005*, ICC-IMB: Essex, pp. 8-9, 2005.
- [16] Andrewatha, A. & Stone, Z., English Maritime Law Update. 35 *J. of Mar. L. & Com.* 369.
- [17] Dixon v. Sadler (1839), 5 *M & W* 414.
- [18] Phipps v. ss Santa Maria, 418 *F.2d* 615-617 (5th. Cir. 1969).
- [19] Rodriguez, A.J. & Hubbard, M.C., The International Safety Management (ISM) Code: A New Level of Uniformity, 73 *Tul. L. Rev.* 1585.
- [20] F.C. Bradley & Sons Ltd. v. Federal Steam Navigation Co. (1926), 24 *L.L.Rep.* 446.
- [21] Moor-Bick, J., The Fjord Wind (1999), 1 *Lloyd's Rep.* 307.
- [22] Clark, J. (2000), 2 *Lloyd's Rep.* 191.
- [23] Cresswell, M.R., The Eurasian Dream (2000), 1 *Lloyd's Rep.* 719.
- [24] LLP, *A Guide to the Hague and Hague-Visby Rules*, LLP: London, 1985.
- [25] The Toledo (1995), 1 *Lloyd's Rep.* 40.
- [26] Hill, Taylor, Dickinson, "ISM Code What if..." *Shipping at a Glance, Guide: 4*, Hill Taylor, Dickinson: London, 2003.
- [27] Norwegian Shipowners' Association (NSA), *Guideline for Performing Ship Security Assessment*, NSA: Oslo, 2003.
- [28] Germanischer Lloyd, *Development and Implementation of a Methodology for the Performance of a Ship Security Assessment*, GL, Hamburg, 2003.
- [29] Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process; IMO Doc. MSC/Circ. 1023, MEPC/Circ. 392, 5 April 2002.
- [30] Guidelines on Places of Refuge for Ships in Need of Assistance; IMO Doc. A23/Res. 949, 5 March 2004.
- [31] Code of Practice on Security in Ports; IMO/ILO, 2005.  
[http://www.imo.org/includes/blastDataOnly.asp/data\\_id%3D8557/ILOIMO\\_CODEDRAFTmesshp-cp-aEnglish.pdf](http://www.imo.org/includes/blastDataOnly.asp/data_id%3D8557/ILOIMO_CODEDRAFTmesshp-cp-aEnglish.pdf)
- [32] Proposal for a Directive of the European Parliament and if the Council on enhancing Port Security; European Commission, 2004.  
[http://europa.eu.int/eur-lex/en/com/pdf/2004/com2004\\_0076en01.pdf](http://europa.eu.int/eur-lex/en/com/pdf/2004/com2004_0076en01.pdf)