

Containerised cargo security - a case for “joined-up” government

Chris Trelawny is the Senior Technical Officer in the Maritime Security Section of the International Maritime Organization (IMO) based in London. He joined IMO in March 2003. From 1997 until 2003, Chris was the Aviation Security Training Officer for the International Civil Aviation Organization (ICAO), based in Montreal. While at ICAO he was responsible for developing training and guidance material for aviation security (AVSEC), including the ICAO training programme for air cargo security. Before joining ICAO, Chris worked for four years as an aviation security inspector for the UK Government, specialising in cargo operations. Prior to that, he spent eight years with HM Customs & Excise, in both aviation and maritime environments.

The views expressed in this article are those of the author. They are designed to promote discussion and should not be taken as a reflection of the views of any of the above-mentioned organizations.

Introduction

Not only did the devastating terrorist acts of 11 September 2001 in the United States accelerate the development and adoption of maritime security procedures by the International Maritime Organization (IMO), they also raised the spectre of terrorist organizations using ships as weapons *per se*, or as delivery systems for weapons of mass destruction (WMD). Nightmare scenarios of “dirty bombs” and biological agents in containers, or LNG, LPG or chemical carriers being triggered to explode in ports of destination, gained in credibility.

However, it is important to bear in mind that containerised cargo security systems and procedures should not just be concerned with the prevention of terrorist acts. Losses through theft of cargo amount to billions of dollars per year and the costs must ultimately be borne by customers and end users through increased insurance and transportation costs. Seafarers’ lives and ships are lost and environments are damaged through the transportation of undeclared, improperly described and badly packed dangerous goods. The trafficking of illicit drugs arguably kills more people and has a far more detrimental effect on society over time than terrorist attacks. The smuggling and diversion of weapons in contravention of national laws and internationally agreed arms embargoes; the illegal migration and trafficking of men, women and children; and the smuggling of nuclear materials and precursors for WMD are all challenges that need to be addressed. If we factor into this mixture the wider issues of protection of national revenues, environmental and cultural concerns, and the need to deprive terrorist organizations of funding, it becomes clear that a co-ordinated approach to cargo security is necessary.

*[Purists will already be muttering that many of the measures to counter the above are facilitation issues, not security issues, and probably won’t read much further. The more enlightened will be recalling worthy phrases such as “security and facilitation are two sides of the same coin” (I have used that one). However, at risk of alienating everybody, let’s go one step further. If we can accept that facilitation is the streamlining of all necessary procedures required by governments; and that these procedures include revenue protection, immigration controls, prevention of smuggling and contraband et cetera **and** security; then security becomes another subset of facilitation and the case for “joined up government” becomes more compelling].*

IMO “Special measures to enhance maritime security”

IMO’s response to “9/11” was swift and dramatic. The Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, held in London in December 2002, adopted amendments to SOLAS, specifically the new chapter XI-2 on “Special measures to enhance maritime security”, and the International Ship and Port Facility Security (ISPS) Code. The new regulatory regime entered into force on 1 July 2004.

These maritime security regulations were developed on the basic understanding that ensuring the security of ships and port facilities was a risk management activity. In order to determine which security measures would be appropriate, an assessment of the risks must be made in each particular case. The purpose of the ISPS Code was to provide Governments with a standardized,

consistent framework for evaluating and managing risk, enabling them to offset changes in threat levels with appropriate measures to address vulnerability for ships and port facilities.

The provisions of SOLAS chapter XI-2 and the ISPS Code were complementary to the guidance previously issued by IMO on combating acts of piracy and armed robbery against ships; the allocation of responsibilities to seek the successful resolution of stowaway cases; and the prevention and suppression of the smuggling of drugs, psychotropic substances and precursor chemicals on ships.

The special measures to enhance maritime security were also complementary to the provisions of the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention), an instrument developed following the 1985 hijacking of the *Achille Lauro*, and primarily aimed at protecting ships. The SUA Convention seeks to ensure that appropriate action is taken against persons committing unlawful acts against ships, including the seizure of ships by force; acts of violence against persons on board ships; and the placing of devices on board a ship which are likely to destroy or damage it. In the context of maritime cargo security, it is of great significance that the SUA Convention has been revised with a new Protocol incorporating new offences and provisions in relation to the transport of WMD and precursors as well as for boarding suspect ships.

Containerised cargo security

The security of maritime cargo and, in particular, containerised maritime cargo, poses challenges from both the legislative and technical viewpoints. As the competent body for all aspects of maritime transportation, IMO took the pragmatic decision to link the new security regime to SOLAS rather than to develop a new instrument mainly because that was the quickest way of introducing effective measures. (The SUA Convention was introduced in 1988 in response to the *Achille Lauro* incident in October 1985. It gained legal force in March 1992, over six years after the event that triggered it, and twenty years (June 2005) later was applicable to 121 States. On the other hand, on 1 July 2004, SOLAS chapter XI-2 and the ISPS code became applicable in 153 States (now 156), i.e. within three years of the events that triggered their adoption).

The trade-off for the time gained in linking maritime security to SOLAS was that SOLAS has limited jurisdiction on land. (As its name implies, it is concerned with the safety of life at sea). As most of the security sensitive parts of the cargo operation take place on land, either in the port area or further inland, it was clear that other vehicles for addressing cargo and container security needed to be found. The 2002 SOLAS Conference therefore passed resolutions on the enhancement of security in co-operation with the International Labour Organization (ILO) and the World Customs Organization (WCO) to broaden the scope of the maritime security regime ashore.

The co-operation with the ILO has led, amongst other things, to the development of the ILO/IMO Code of practice on security in ports. Not only does this useful document extend the functional requirements of the ISPS Code into the wider port area, thus addressing some aspects of cargo security, it also provides guidance on effective co-operation, co-ordination and communication of security, as well as a practical methodology for threat and risk assessment.

WCO “Framework of Standards to secure and facilitate global trade”

Of even greater significance to container security was the co-operation with the WCO. The WCO was requested to consider urgently measures to enhance security throughout international movements of closed cargo transport units (closed CTUs). Operative paragraph 3 of Conference resolution 9 “*agrees that the [SOLAS] Convention should be amended, if and when appropriate, to give effect to relevant decisions taken by the WCO and endorsed by the Contracting Governments to the Convention insofar as these relate to the carriage of closed CTUs by sea*”.

In June 2004, the WCO Council tasked an *ad hoc* High Level Strategic Group of the representative Directors General of Customs from across all WCO regions to draw together by June 2005, the measures and instruments to enhance the security of the international supply chain which the WCO Task Force developed between June 2002 and April 2003, into a Framework of Standards to secure and facilitate global trade (the Framework of Standards).

The Framework of Standards was developed with four principles in mind, namely that Customs services would undertake to harmonize advance electronic information; to use a consistent risk management approach; use non-intrusive detection equipment; and lead to the accrual of benefits to customs, business and ultimately nations. At its heart were two ‘pillars’, the Customs-to-Customs pillar and the Customs-to-Business pillar, each of which is supported by broadly defined outline standards. The Framework of Standards was unanimously adopted by Directors General of 166 Customs Administrations meeting at the 105th/106th Sessions of the WCO Council, held in Brussels from 23 to 25 June 2005.

The Framework of Standards, *per se*, is the start of the process and specific standards on cargo security will need to be developed and agreed. The WCO believes that implementation of the Framework of Standards measures will assist security and customs authorities to enhance their risk assessment capabilities and therefore adopt a “smarter” approach to targeting closed CTUs for inspection. As this activity will be primarily based on assessment of documentation and confirmation of the integrity of supply chain security, it is unlikely to have an appreciable effect on the way that containers are physically handled, but it may enhance the speed with which they are cleared for shipment.

There are compelling arguments for using customs authorities in the security process. As the WCO Framework of Standards document points out: “Customs administrations have important powers that exist nowhere else in government - the authority to inspect cargo and goods shipped into, through and out of a country. Customs also have the authority to refuse entry or exit and the authority to expedite entry. Customs administrations require information about goods being imported, and often require information about goods exported. They can, with appropriate legislation, require that information to be provided in advance and electronically. Given the unique authorities and expertise, Customs can and should play a central role in the security and facilitation of global trade. However, a holistic approach is required to optimize the securing of the international trade supply chain while ensuring continued improvements in trade facilitation. Customs should therefore be encouraged to develop co-operative arrangements with other government agencies”.¹ It is these co-operative arrangements that are the key to success in maritime cargo security.

Technical challenges in container security

One of the main challenges to using customs authorities in the cargo security role is their operational culture. Customs have traditionally been more focussed on what is coming into the country rather than what is going out. Whereas this works well for revenue protection and detection of contraband, if maritime security measures are to be effective, they must be implemented prior to departure rather than at the point of arrival. Put simply, if a ship carrying a containerised dirty bomb is not subject to security control until it reaches the port of destination, it may well be too late. Similarly, many traditional maritime control procedures required under SOLAS, for example port State control for safety purposes, are also concentrated on the point of arrival. Some international programmes, for example the United States’ Container Security Initiative (CSI) (and to a certain extent the overseas end of the Customs - Trade Partnership Against Terrorism (C-TPAT)) have sought to address this issue by transferring the onus to security checks to the point of departure. This, issues of extra-territoriality and sovereignty

¹ Framework of standards to secure and facilitate global trade paragraph 1.1 (see <http://www.wcoomd.org>)

notwithstanding, is a step in the right direction and echoes the aviation model of “host State responsibility”.

Any cargo security system must involve a considerable degree of liaison between the security practitioners and customs authorities, at least at the policy and legal levels. In many States international cargo travels under customs bond. Many storage and loading areas in ports and port facilities are customs controlled areas. What therefore are the legal implications for a port facility or ship security officer who wishes to check the contents of a container?

Even once the issue of legal right of access has been settled and procedures have been agreed, there is also the whole issue of facilitation and co-ordination of inspection between the various control authorities. Opening a container for inspection by customs, re-sealing it, opening it for inspection by port health authorities, re-sealing it, opening it for inspection by security, resealing it and so on, would be extremely inefficient and time consuming and therefore delaying. Such practices would also leave little chance of maintaining a credible audit trail for security purposes and would also considerably increase the chances of the ill-disposed (be they corrupt officials or otherwise) adding to or depleting, the contents of the container.

The key question is which containers need to be checked, and for what? One thing is certain, that you cannot screen them all effectively. From a counter-terrorist security perspective, clearly a box from a reputable, regular consignor to a reputable consignee, packed in secure conditions, demonstrably kept secure thereafter and with correct documentation, merits less attention than a one-off shipment from an unknown source. The need for an accurate assessment of the threat is clear. From a counter-terrorist perspective, “gathering and assessing information with respect to security threats” is a functional requirement of the ISPS Code.² But what about the other concerns: drugs, dangerous goods, endangered species, agricultural health etc? How can meaningful threat assessments from a number of different sources and addressing all of these concerns be co-ordinated and acted upon, without bringing world maritime trade to shuddering halt?

The whole concept of the application of security to containers at the port or port facility also warrants further investigation. The champions of high-technology solutions, usually the manufacturers, their agents and politicians seduced by persuasive glossy brochures and secure employment in their constituencies, would have us believe that container screening systems at ports and port facilities, coupled with the use smart seals, and transponders and detection systems in every container, will secure the maritime supply chain. However, the reality is that even if the State of export could afford such equipment, the sheer volume of cargo being shipped limits its use to a small percentage of containers being shipped, with clearly defined parameters of which threat / irregularity to look for.

The regulated agent concept

Surely the logical solution to all of this is a partnership between Governments, all of the control authorities and security agencies with an interest in maritime cargo, the consignors, companies and cargo handling agents.

The logical place to apply the security is at the source, i.e. where the containers are stuffed. Once the contents have been established as being correct, non-threatening and legal, procedural security measures such as the use of seals, control of access, correct documentation and verifiable handling procedures can be applied. This then removes the need for further screening or searching of the containers at the port or port facility, except on a random sampling basis.

² ISPS Code part A/1.3.1

The Governmental buy-in to this would be in the form of national legislation empowering control authorities to delegate some of their functions to the consignors and/or cargo handling agents, through the application of agreed cargo security plans. This would have to be matched with appropriate powers for the control authorities to oversee compliance with the agreed plans by the “regulated agents”.

The benefit to the industry of such an approach could be that regulated agents would be able to “fast track” their containers through export controls. The threat of losing regulated agent status, thus losing economic benefits of the fast track facility, should be enough incentive to maintain compliance by the shippers. The benefits to the control authorities would be a ready-made risk assessment process, thus allowing them to concentrate on the higher risk exporters who do not qualify for regulated agent status, coupled with an auditable trail for investigating irregularities.

The regulation process could vary in complexity according to the individual national need. For example, individual agents could be regulated in respect of security, customs and revenue (“approved economic operators” in WCO parlance), carriage of dangerous goods, licensable goods, etc, or any combination thereof.

As a further incentive for compliance, and using the WCO’s “customs-to-customs” model, importing States could also “fast track” clearance of consignments received from regulated agents, subject to the regulated having a clean record. Any irregularities found by control authorities in the importing State during the course of random inspection, could be referred back to the relevant control authorities in the originating State.

Summary

The implementation, by Governments, of a regulated agent system for maritime supply chain security, based upon the WCO Framework of Standards model, could have significant benefits for increasing safety and security while at the same time enhancing the facilitation of international trade. Procedural security measures, consistent with the approach of ISO, would enhance the effectiveness of such an approach, while at the same time building confidence in the integrity of the system. For such a system to work will require the commitment of all Government agencies concerned with cross-border controls and security.