Manuel Gómez Martín

Overview of the Protection Methods Applied to Maritime Transport
Visión global de las medidas de protección aplicadas al transporte marítimo

El terrorismo contra medios de transporte no es un fenómeno nuevo, y tampoco lo son las acciones terroristas específicamente dirigidas a medios de transporte marítimo.

Achille Lauro

Quizás el primer incidente que hizo reaccionar a los organismos internacionales, fue el secuestro del buque Achille Lauro, que tuvo lugar el 7 de Octubre de 1985. Ese día, cinco terroristas armados secuestraron el buque de cruceros italiano, con 400 personas abordo, reclamando la libertad de 50 prisioneros palestinos. Se produjo únicamente una víctima, Leon Klinhoffer, un americano de 69 años, inválido, que fue arrojado por la borda en su silla de ruedas. El Achille Lauro había hecho escala en Port Said y se dirigía a Alejandría.

El buque tenía 193 metros de eslora, 25 metros de manga y 8.5 metros de calado. Su arqueo superaba las 23.000 toneladas y era capaz de transportar 1.600 pasajeros a una velocidad máxima de 22 nudos. El Achille Lauro ya había tenido una vida agitada desde sus inicios. Se comenzó su construcción en los Países Bajos en 1939, pero se paralizó con el inicio de la Guerra Mundial. Fue bombardeado por las tropas alemanas, quienes reiniciaron su construcción, que fue saboteada por la resistencia holandesa y nuevamente bombardeado, esta vez por la RAF, y abandonado. En 1946 fue botado y entregado a su Armador, Rotterdamsche Lloyd, que lo dedicó a la línea entre Países Bajos e Indonesia.

Como consecuencia de la disminución de tráficos debido a la independencia de Indonesia, el buque fue dedicado al tráfico con Estados Unidos, poco después de colisionar con su buque rival, el Oranje de la Nederland Line.

El buque fue vendido a Lauro Line en 1965, sufrió una explosión e incendio durante su reacondicionamiento en un astillero en Sicilia, y en 1972 fue dedicado a cruceros, sufriendo al menos una

Terrorism against modes of transport is not a new phenomenon, nor are terrorist activities specifically aimed at any type of maritime transport.

Achille Lauro

Perhaps the first incident of this kind that made international organisations react, was the seizure of the vessel Achille Lauro, which took place on October 7th, 1985. On that particular day, five armed terrorists seized the Italian ship with 400 people on board, demanding that 50 Palestinian prisoners be released from jail. There was only one victim on this occasion, Leon Klinghoffer, a 69-year old handicapped U.S. citizen, who was thrown overboard in his wheelchair. Port Said was one of the Achille Lauro's ports of call and it was bound for Alexandria.

The vessel was 193 metres long, 25 metres wide and had a draught of 8.5 metres. Its tonnage was in excess of 23,000 tonnes and it could transport 1,600 passengers at a maximum speed of 22 knots. Ever since it entered service the Achille Lauro had a problematic existence. Construction began on the ship in the Netherlands in 1939, but activities came to a halt when World War II broke out. It was bombed by German troops, who then resumed the construction process. However, the Dutch Resistance sabotaged the work, before it was once again bombed, this time by the RAF, after which it was abandoned. It was eventually launched in 1946 and handed over to its owner, Rotterdam Lloyd, which put it into service on the line running from the Netherlands to Indonesia.

As a result of reduced traffic due to Indonesian independence, the vessel was used for traffic with the United States, until it collided with the Oranje, its competitor from the Nederland Line.

The ship was sold to the Lauro Line in 1965, but there was an explosion on board and it caught fire during maintenance at a Sicilian shipyard. In 1972 it was used as a cruise ship, and while being employed for this purpose it had at least one collision with a vessel transporting livestock, and caught fire twice, the last time in 1994 off the coast of Somalia, with 1,090 passengers on board; it was completely destroyed on this occasion.

The SUA Agreement

On November 20th 1985, immediately after the seizure, at the General Assembly of the International Maritime Organisation (IMO), a decision was reached (Resolution A.584 [14]) urging that measures be taken to prevent illegal acts that threatened vessel safety / security and to safeguard their passage and crew members.

As a result of this Resolution, the IMO proceeded to work towards this aim and, on March 10th 1988, the Organisation adopted the measure with a view to controlling illegal acts that jeopardised the security of maritime navigation (SUA, Suppression of Unlawful Acts), as an extension to the provisions contained in the Protocol for the repression of illegal acts committed against the safety/security of oil rigs located on the continental shelf, which was passed that same year.

The SUA Agreement guarantees that suitable measures will be taken against vessels who commit illegal acts against seafaring vessel, including the following:

¬ When a vessel is forcibly taken over, by violent means or through the threat of violence or any other kind of intimidation;

¬ Violence against people on board a ship;

¬ Destruction of or damage done to a vessel or to its cargo that could jeopardise safe navigation;

¬ Planting explosive devices or products on a vessel that could destroy it, damage it or cause damage to the cargo that jeopardises safe navigation;

¬ Destroying or damaging maritime navigation equipment, facilities or services that might cause safe navigation to be put at risk.

Furthermore, action shall be taken against those who commit the crime of disclosing false information that exposes navigation to danger, or leads to death or injury.

The Agreement, which is currently being updated by the IMO Legal Committee, includes the imposition of penalties on and/or the extradition of persons who have committed the aforementioned criminal acts.

Maritime Transport 'Post 9/11'

However, it is undoubtedly the case that the events that did most to change Government awareness and sensitivity regarding the vulnerability to organised terrorist groups willing to kill thousands of people to achieve their aims, were the devastating attacks perpetrated on September 11th 2001 in New York and Washington. The risk of mega-terrorism was no longer merely a storyline for a novel but had now become an unexpected reality, and the world maritime transport system was now regarded as a target or a vehicle for future terrorist attacks.

As the OCDE Maritime Transport Committee quite rightly pointed out in its report on the security of maritime transport published in 2003, world trade depends on maritime transport to a large extent. However, the same specific features of this mode of transport that have been vital to economic growth are extremely vulnerable if they are targeted by terrorist groups to further their interests. Such weaknesses include interfering with items of cargo or ships themselves, falsifying documents or raising funds for illegal purposes. Unfortunately, taking such preventive measures against the consequences of terrorist activity in order to protect international maritime transport would have major repercussions on the world economy.

During the second half of the 20th Century, great progress was made where world prosperity was concerned, and this was enhanced by the freedom of movement of goods. The removal of trade barriers and a reduction in transport costs made it possible to develop a global and interrelated economy. Manufacturers and distributors alike developed processes that enabled them to reduce stocks to a minimum, helped by rapid and efficient transport systems. This scenario changed on September 11th 2001 when, as a result of the attacks on the Twin Towers of the World Trade Center in New York, the United States, - for the first time in its history -, closed its air space to commercial aviation. Although maritime transport was the subject of tighter security measures, it was not affected by the events, apart from the temporary closure of some facilities in the vicinity of New York or the detention of a particular vessel.

Maritime Transport and Terrorist Threat

The terrorist risk factors involved in maritime transport can be split into the following categories:

1. *Associated with cargo*:
¬ Illegal boarding of persons or weapons;
¬ Transporting conventional weapons, or NCB, (nuclear, chemical or biological weapons).
2. *Associated with vessels*:
¬ Use of a vessel as a weapon;
¬ Use of a vessel as the base for launching an attack;
¬ Sinking a vessel to prevent navigation.
3. *Associated with people*:
¬ Attacking a vessel to cause injury to people;
¬ Terrorists boarding under the guise of crew members.
4. *Associated with financing*:
¬ Use of income from maritime business to finance terrorist activities;
¬ Using vessels to obtain illegal funds for terrorist groups;
5. *Associated with external impact*:
¬ Loss of human life and damage to property;
¬ Interruption to the flow of goods;
¬ Increasing transport costs by taking additional security measures.

Take the worst possible scenario, in which a terrorist group manages to place weapons of mass destruction activated by satellite in a maritime container, inserting them in the international transport chain using shippers, transport contractors and legal agents, to activate the device by remote control when the container is in a major population centre. This operation could be carried out only with the weapons concerned, plus a minimal knowledge of international transportation practice.

The possibility of an attack of this nature is revealed only when a small number of containers are subjected to an inspection of this type. In the United States, before the World Trade Center attacks, only about 2% of the containers that entered the USA were inspected.

Fears that terrorists might use the container transportation system to achieve their ends were confirmed on October 18th 2001, only 37 days after the attacks in New York and Washington, when the Gioia Tauro Port Authorities found a stowaway in a container. The container had been boarded at Port Said, for shipment to the Italian port in a vessel heading for Rotterdam, where it was to be transferred to a ship bound for Canada.

The stowaway was found by the Harbour Police, as a result of sounds coming from the container, apparently when the stowaway tried to increase the amount of fresh air coming in through the ventilator. The container had been painted and labeled as a container belonging to Maersk, which had been replaced.

The vessel that had transported it as far as Gioia Tauro was the Ipex Emperor, owned by Andrew Weir, chartered by Maersk, constructed in Germany in 1966, 210 metres long with a capacity of 3,000 TEUs.

The stowaway, Rigk Amed Farid, was born in Egypt, and held a Canadian passport. He was accused of international terrorism under Article 270 of the Italian Penal Code, and released on bail following application from his defence lawyer midway through November 2001, but he disappeared before more information could be gathered about him.

The container was equipped with a bed a heater, a toilet and water tanks. The stowaway had a mobile phone, and a second phone that was able to communicate via satellite, a laptop computer, airport security passes, certificates showing he was a qualified airline mechanic,

colisión con un buque transporte de ganado y dos incendios, el último en 1994, en las costas de Somalia, con 1.090 pasajeros abordo, quedando totalmente destruido.

El Convenio SUA

El día 20 de Noviembre de 1985, inmediatamente después del secuestro, la Asamblea de IMO, Organización Marítima Internacional, adoptó la Resolución A.584 (14), que insta a que se elaboren medidas para prevenir los actos ilícitos que amenazan la seguridad del buque y la salvaguardia de su pasaje y tripulación.

Como consecuencia de esta Resolución, IMO continuó trabajando en este mismo sentido y adoptó, el 10 de Marzo de 1988, el Convenio contra la represión de actos ilícitos contra la seguridad en la navegación marítima (SUA, Suppression of Unlawful Acts), como estensión de las previsiones del Protocolo para la represión de actos ilícitos contra la seguridad de las plataformas localizadas en la plataforma continental de ese mismo año.

El Convenio SUA garantiza la adopción de medidas adecuadas contra las personas que cometan actos ilícitos contra los buques, incluyendo:

¬ El secuestro de un buque por la fuerza o su control mediante violencia, amenaza de violencia o cualquier tipo de intimidación;
¬ La violencia contra personas a bordo de un buque;
¬ La destrucción o daños al buque o a su carga que puedan poner en peligro la navegación segura;
¬ La colocación en un buque de artefactos o productos que puedan destruirlo o dañarlo o provocar daños a la carga que pongan en peligro su segura navegación;
¬ La destrucción o daños en instalaciones o servicios de navegación marítima si se pone en peligro la navegación segura.

Igualmente se procederá contra aquéllos que difundan información falsa que ponga en peligro la navegación de un buque y a quien mate o lesione a cualquier persona en relación con la comisión de los delitos antes descritos.

El Convenio, que se encuentra actualmente en revisión por el Comité Legal de IMO, prevé la aplicación de penas y la extradición de las personas que hayan cometido los actos delictivos referidos.

El transporte marítimo 'post 9-11'

Pero no existe duda de que los sucesos que cambiaron la sensibilidad de los Gobiernos sobre la vulnerabilidad frente a grupos terroristas organizados, dispuestos a sacrificar miles de vidas para conseguir sus objetivos, fueron los devastadores ataques del día 11 de Septiembre de 2001 en Nueva York y Washington. El riesgo de mega-terrorismo pasó de ser una idea para el guión de una novela a convertirse en un hecho real insospechado, y el sistema mundial de transporte marítimo pasó a ser considerado como blanco o como vehículo de futuros ataques terroristas.

Como acertadamente apunta el informe del Comité de Transporte Marítimo de OCDE sobre la seguridad del transporte marítimo publicado en 2003, el comercio mundial depende en gran medida del transporte marítimo. Pero las mismas particularidades de este medio que han sido claves para el crecimiento económico suponen su gran vulnerabilidad si son aprovechadas por grupos terroristas para favorecer sus iniciativas. Estas debilidades incluyen la intromisión en partidas de carga o en buques, el fraude documental o la generación de fondos con fines ilegales. Desgraciadamente, las consecuencias de una interrupción en el transporte marítimo internacional afectarían de modo importante a la economía mundial.

Durante la segunda mitad del siglo pasado los importantes avances en la prosperidad del mundo han estado propiciados por la libertad en el movimiento de mercancías. La desaparición de las

barreras al libre comercio y la reducción de las tarifas de transporte han posibilitado el desarrollo de una economía global e inter-relacionada. Los fabricantes y los distribuidores han desarrollado procesos que permiten reducir al mínimo los stocks, ayudados por sistemas de transporte rápidos y eficientes.
Este escenario cambió el 11 de Septiembre de 2001 cuando, como consecuencia de los ataques a las Torres Gemelas de Nueva York, los Estados Unidos, por primera vez en su historia, cerraron su espacio aéreo a la aviación comercial. El transporte marítimo, aunque fue objeto de mayores medidas de seguridad, no fue afectado por estos sucesos, si exceptuamos el cierre temporal de alguna instalación en la zona de Nueva York o la detención puntual de algún buque.

Transporte marítimo y riesgo terrorista

Los factores de riesgo terrorista relacionados con el transporte marítimo se pueden dividir como sigue:
1. *Relacionados con la carga*:
¬ Introducción ilegal de personas o armamento;
¬ Transporte de armas convencionales, ó NCB, (armas nucleares, químicas o biológicas).
2. *Relacionados con el buque*:
¬ Utilización de un buque como arma;
¬ Utilización de un buque como base para lanzar un ataque;
¬ Hundimiento de un buque para imposibilitar el tráfico.
3. *Relacionados con las personas*:
¬ Atacar a un buque para provocar daños a las personas;
¬ Introducir a terroristas bajo la identidad de tripulantes.
4. *Relacionados con la financiación*:
¬ Utilización de los ingresos del negocio marítimo para financiar actividades terroristas;
¬ Utilizar los buques para obtener fondos ilícitos para grupos terroristas.
5. *Relacionadas con el impacto externo*:
¬ Pérdida de vidas humanas y daños a las propiedades;
¬ Interrupción de los flujos de mercancías;
¬ Incremento en los costos de transporte debido a las medidas de seguridad adicionales.
Se puede considerar el peor de los escenarios, en el que un grupo terrorista podría colocar armas de destrucción masiva activables por vía satélite en un contenedor marítimo e introducirlo en la cadena de transporte internacional utilizando embarcadores, transportistas e intermediarios legales, para activar el dispositivo a distancia cuando el contenedor se encontrase en un gran centro de población. Para realizar esta operación se necesitarían únicamente el arma y unos conocimientos mínimos de las prácticas del transporte internacional.
La posibilidad de una actuación de este tipo se pone de manifiesto cuando solamente se somete a inspección física una parte muy pequeña de los contenedores. En los Estados Unidos, con anterioridad a los ataques al World Trade Center, aproximadamente el 2% de los contenedores que entraban en USA eran inspeccionados.
Los temores de que los terroristas pudieran utilizar para sus fines los sistemas de transporte de contenedores se confirmaron el día 18 de Octubre de 2001, solamente 37 días después de los ataques en Nueva York y Washington, cuando la Autoridad Portuaria de Gioia Tauro descubrió un polizón en un contenedor. El contenedor había sido embarcado en Port Said, para transbordo en el puerto italiano en un buque con destino Rotterdam, donde sería nuevamente transbordado con destino final Canadá.
El descubrimiento del polizón lo realiza la Policía Portuaria, como consecuencia de los sonidos producidos en el contenedor, al parecer cuando el polizón intentaba aumentar la entrada de aire fresco a través del ventilador. El contenedor había sido pintado y marcado como un contenedor de Maersk, al que había reemplazado.
El buque que lo había transportado hasta Gioia Tauro era el Ipex Emperor, propiedad de Andrew Weir, fletado por Maersk, construido en Alemania en 1966, de 210 metros de eslora y 3.000 Teus de capacidad.
El polizón, Rigk Amed Farid, era egipcio de nacimiento, con pasaporte canadiense. Fue acusado de terrorismo internacional de acuerdo al artículo 270 del Código Penal Italiano, fue puesto en libertad bajo fianza a petición de su abogado defensor a mediados de noviembre de 2001, y desapareció antes de que se pudiera obtener más información.
El contenedor estaba equipado con una cama, un calentador, un WC y depósitos de agua. El polizón disponía de un teléfono móvil, un teléfono vía satélite, un ordenador portátil, y pases de seguridad aeroportuaria y certificados de mecánico de línea aérea, con acceso a pista, válidos para los aeropuertos de JFK en Nueva York, Newark en Nueva Jersey, Los Angeles International Airport y Chicago O'Hare.

C-TPAT

Tal como ocurrió como reacción al secuestro del buque Achille

and runway access passes that were valid for the following airports: JFK in New York, Newark in New Jersey, Los Angeles International Airport and Chicago O'Hare.

C-TPAT

As was the case with the reaction to the seizure of the Achille Lauro, when the IMO passed Resolution A.584 (14) which urged countries to prepare measures to prevent illegal actions that threatened the vessels' security and safeguarded their passage and crew members, immediately after the attacks on the September 11th, a variety of bodies drew up procedures to prevent risks of an antisocial nature that used any of the links in the logistics chain as a target or as a vehicle.
The first of these initiatives was known as the C-TPAT, Customs-Trade Partnership Against Terrorism, which was presented in November 2001, only two months after the terrorist attack. The initiative was developed by the US border agency, CBP, Customs and Border Protection, formerly known as the U.S. Customs Service.
The aim of this programme is to improve the security in the supply chain. The basic principle of this process is voluntary participation and the joint development of security criteria based upon best practices.
If a company wishes to participate in this programme – which was originally limited to American importers, but later applied to all those who are part of the logistics chain –, it first has to submit a report to the CBP containing all the security processes that it has implemented, together with the improvements that it intends to make to those processes in order to be granted the C-TPAT certificate. The company must likewise specify the processes or improved practices that take place in succession throughout the supply chain and proactively guarantee that all the individual members of this chain will take part in those improved practice processes.
The C-TPAT alliance between the company and CBP must include at least the formalisation of the procedures in seven key areas: Physical Security, Access Control, Personnel Security, Document Processes, Appointed, Training and Shipment Security Procedures.

The aim of this initiative is to achieve the following objectives:
¬ To improve the security of a considerable percentage of shipments to the United States;
¬ To give benefits to the private companies that comply with the security criteria in the supply chain;
¬ To enable the CBP to concentrate its inspection resources and capacities on high-risk shipments.
The CBP's great priority is to prevent terrorists and their weapons from entering the United States, and this includes weapons of mass destruction. It establishes the C-TPAT Programme as the most ambitious project yet between the United States Government and the private sector, as a direct result of the events that took place on September11th. The first companies to implement the programme were 7 of the major importers to the USA. Now, 10,200 companies are taking part in the C-TPAT, including 86 of the 100 top American companies that import goods into the United States in containers.
This means that more than 10,000 companies have made or are making major modifications to the security processes in their logistics chains and are requesting that their partners and suppliers do likewise.
Apart from playing an active part in the fight against terrorism, these companies have succeeded in achieving a safer and more secure logistics chain to the benefit of their suppliers, clients and employees. The following are among the numerous benefits to be obtained.
¬ Fewer inspections and shorter delays at the border;
¬ Acceptance by the CBP of a C-TPAT specialist as the only spokesperson with them in matters concerning security, procedures and communications;
¬ C-TPAT importers can gain access to a "fast lane" for entry into the United States.
Furthermore, the logistics chain is more cohesive, which means the following:
¬ Fewer losses due to robbery or theft;
¬ Improvements to the workers' security.
The aim of the initiative is to involve all those involved in the transportation chain, for the purpose of which the CBP has defined eight groups to be included in the certification process. These groups are:

Lauro, con la aprobación por IMO de la resolución A.584 (14) que instaba a los países a elaborar medidas para prevenir los actos ilícitos que amenazan la seguridad del buque y la salvaguardia de su pasaje y tripulación, inmediatamente después de los ataques del 11 de Septiembre diversos organismos desarrollaron procedimientos para prevenir el riesgo de actos de naturaleza antisocial que utilizaran como blanco o como vehículo cualquiera de los eslabones de la cadena logística.
La primera de estas iniciativas fue la denominada C-TPAT, Customs-Trade Partnership Against Terrorism, que se presentó en Noviembre de 2001, solamente dos meses después del ataque terrorista. La iniciativa ha sido desarrollada por la agencia de fronteras de los Estados Unidos, CBP, Customs and Border Protection, anteriormente denominada U.S. Customs Service.
El objetivo del programa es mejorar la seguridad en la cadena de suministro. El principio fundamental de este proceso es la participación voluntaria y el desarrollo conjunto de criterios de seguridad basados en las mejores prácticas.
Para participar en este proograma, que inicialmente estaba limitado a los importadores americanos, pero que posteriormente se extendió a todos los participantes en la cadena logística, la empresa debe presentar a CBP una memoria de los procesos de seguridad que tiene implantados, y aquellas mejoras de esos procesos que se compromete a realizar para obtener el certificado C-TPAT. La empresa deberá indicar los procesos o mejores prácticas que se producen en cascada a lo largo de la cadena de suministro y garantizar de forma pro-activa que todos los miembros individuales de esa cadena participarán en esos procesos de mejores prácticas.
La alianza C-TPAT entre la empresa y CBP debe incluir, como mínimo, la formalización de procedimientos en siete áreas clave: Seguridad física, Control de accesos, Seguridad del personal, Procesos documentarios, Procedimientos de manifiesto, Formación y Seguridad en los envíos.
Esta iniciativa está diseñada para lograr estas metas:
¬ Mejorar la seguridad de un importante porcentaje de embarques hacia los Estados Unidos;
¬ Conceder beneficios a las compañías privadas que cumplan con los criterios de seguridad en la cadena de suministro;
¬ Concentrar los recursos y capacidades de inspección del CBP en los embarques de alto riesgo.
CBP tiene como misión prioritaria impedir la entrada en los Estados Unidos a terroristas y armamento terrorista, incluidas las armas de destrucción masiva. Define al Programa C-TPAT como el más ambicioso proyecto de colaboración entre el Gobierno de los Estados Unidos y el sector privado como consecuencia de los sucesos del 11 de Septiembre. Inicialmente se adhirieron al programa 7 de los mayores importadores de USA. Hoy participan en C-TPAT 10.200 compañías, entre las que se encuentran 86 de las 100 mayores empresas americanas importadoras de mercancía en contenedor en los Estados Unidos.
Esto significa que más de 10.000 empresas han realizado o están realizando revisiones profundas de los procesos de seguridad en sus cadenas logísticas y solicitando a sus socios y proveedores que se adhieran a prácticas similares.
Estas empresas, además de desempeñar un papel activo en la lucha contra el terrorismo, consiguen una cadena logística más segura en beneficio de sus proveedores, clientes y empleados.
Entre otros muchos, se pueden enumerar los siguientes beneficios:
¬ Menor número de inspecciones y menores esperas en frontera;
¬ Aceptación por parte de CBP de un especialista C-TPAT como interlocutor único con ellos en temas relacionados con la seguridad, los procedimientos y las comunicaciones;
¬ Los importadores C-TPAT pueden acceder a un canal rápido de entrada en los Estados Unidos.
Adicionalmente, se consigue una mayor integridad de la cadena logística, lo que permite:
¬ Menores pérdidas por hurtos o robos;
¬ Mejoras de seguridad para los trabajadores.
La iniciativa pretende involucrar a todos los actores de la cadena de transporte, para lo que CBP ha definido ocho grupos para ser incluidos en el proceso de certificación. Estos grupos son: importadores, navieros, transportistas aéreos, transportistas ferroviarios, NVOCC/Consolidadores, Operadores de terminales marítimas, Agentes de aduanas y Fabricantes extranjeros.
En resumen, el programa C-TPAT permite a la Aduana reconocer a ciertas compañías como de bajo riesgo, y por tanto con menor necesidad de ser inspeccionadas. Este reconocimiento se basa en el historial de cumplimiento con la Aduana, en su perfil de seguridad y en la validación de su cadena logística.

Container Security Initiative – C.S.I.

Esta iniciativa fue puesta en marcha igualmente por el U.S. Customs, actualmente Customs and Border Protection, perteneciente al U.S. Department of Homeland Security, como consecuencia de los ataques terroristas del 11 de Septiembre, y tiene

importers, ship owners, air transporters, rail transporters, NVOCC/Consolidators, Maritime Terminal Operators, Customs Officers and Foreign Manufacturers.
In summary, the C-TPAT programme enables the Customs to identify certain companies as being low risk, as companies that do not need to be inspected to such an extent. This recognition is based on their background of compliance with Customs, their security profile and on the endorsement of their logistics chain.

Container Security Initiative – C.S.I.
This initiative was also put into practice by the U.S. Customs, now known as Customs and Border Protection, answerable to the U.S. Department of Homeland Security, as a result of the September 11th terrorist attacks, and its most pressing aim is to protect the transport systems and the corridors between the foreign ports to which it applies and the United States. Its aim is to ensure that the inspections carried out in the USA are the final protection barrier against terrorist activities, and not the only barrier, so controls are established before the containers depart from the container vessels' final port of call before they leave for the United States.
This programme was launched in 2002, and it mainly aims to implement these measures in the 20 leading ports that deal with containers heading for the United States. It was formalised through agreements between the American Customs and the Customs in the countries where the ports participating in the initiative are located. In the CSI programme, a team of CBP officials go to the host country to work together with local Customs in detecting the containers that amount to a potential risk. At present, the CSI programme is being applied to other ports as well as the aforementioned original ones. In 2005, 37 ports in 20 countries were at different phases in the process of implementing the initiative. Furthermore, China and Sri Lanka had signed Declarations of Principles (DOP) with US Customs with a view to adhering to the CSI Programme.
There is also a reciprocal programme, whereby the CSI offers participating countries the possibility of sending their own customs officers to ports in the United States to jointly analyse and identify the containerised cargos that are exported to their countries. As part of this reciprocal agreement, Canada and Japan have customs officers in US ports as part of the CSI programme.
The idea of putting this initiative into practice is based on the fact that 90% of cargo is shipped in containers, and that 50% of American imports (in value) enter the United States in containers by sea.
The key factors of the initiative are as follows:
¬ Use of intelligence and automated information to spot and locate containers that could pose a terrorist threat;
¬ Pre-inspection of those containers that are considered to be a risk in the port of origin, i.e. before they reach the USA;
¬ Use of sophisticated detection technologies to rapidly pre-inspect suspect containers;
¬ Use of 'intelligent containers' that can detect undue manipulation.
This programme operates in the following way:
¬ The US CBP and the host Government collaborate in detecting high-risk containers, which they then select for pre-inspection;
¬ The host Government must be able to rely on non-intrusive inspection equipment for the containers;
¬ If the non-intrusive inspection does not yield satisfactory results, the host Government Customs physically inspects the container, while the CBP acts in the capacity of observers…
¬ Any high-risk containers or those that have been subjected to pre-inspection or physical inspection with satisfactory results can enter the United States without delay.
The aim of these measures is to increase security without imposing any restrictions on legal trade.

C.S.I. in Spain
At the time when the initiative was launched, only the Port of Algeciras was included among those that could take part in the C.S.I. programme, which is undoubtedly a disadvantage to the Ports of Barcelona and Valencia, because both have major traffic with the United States. That is why the agreement signed between the CBP and the Spanish Customs included all three ports in the programme. The requirements imposed by

como objetivo prioritario la protección de los sistemas de transporte y de los corredores entre los puertos extranjeros a los que se aplica y los Estados Unidos. Pretende que las inspecciones en USA sean la última barrera de protección contra actos terroristas, y no la única, por lo que se establecen controles antes de la salida de los contenedores desde el último puerto que escalan los buques portacontenedores con destino a los Estados Unidos.
Este programa fue lanzado en el año 2002, y destinado inicialmente a su puesta en funcionamiento en los 20 mayores puertos con tráfico de contenedores con Estados Unidos. Se formaliza mediante acuerdos entre la Aduana americana y la Aduana de los gobiernos de los países en los que se encuentran los puertos que participan en la iniciativa. En el programa CSI, un equipo de funcionarios de CBP se traslada al país anfitrión para trabajar conjuntamente con la Aduana local en la detección de aquellos contenedores que supongan un riesgo potencial. Actualmente CSI se extiende a otros puertos además de los inicialmente previstos. En 2005, 37 puertos en 20 países se encontraban en distintas fases del proceso de implantación de la iniciativa. Además, China y Sri Lanka habían firmado Declaraciones de Principio (DOP) con la Aduana americana para integrarse en CSI.
Adicionalmente, existe un programa recíproco, por el cual CSI ofrece a los países participantes la posibilidad de enviar funcionarios de aduanas a los puertos en Estados Unidos para la identificación y el análisis conjunto de la carga contenedorizada que se exporta a sus países. Como parte de esa reciprocidad, Canadá y Japón tienen aduaneros en puertos de Estados Unidos dentro del programa CSI.
La idea de la puesta en marcha de la iniciativa se basa en el hecho de que un 90% de la carga se mueve en contenedor, y que el 50% de las importaciones americanas (en valor) entra en los Estados Unidos en contenedor por vía marítima.
Los factores clave de la iniciativa son los siguientes:
¬ Uso de la inteligencia y de la información automatizada para identificar y localizar los contenedores que pudieran suponer un riesgo de terrorismo;
¬ Pre-inspección de aquellos contenedores que se consideren de riesgo en el puerto de origen, por tanto con anterioridad a su llegada a USA;
¬ Utilización de tecnologías avanzadas de detección para la rápida pre-inspección de los contenedores sospechosos;
¬ Utilización de 'contenedores inteligentes' que detecten manipulaciones indebidas.
El modo en que funciona el programa es:
¬ El US CBP y el Gobierno anfitrión colaboran para la detección de contenedores de alto riesgo, a los que se selecciona para pre-inspección;
¬ El Gobierno anfitrión debe contar con equipos de inspección no intrusiva de contenedores;
¬ En el caso de que la inspección no intrusiva no sea satisfactoria, se procede a la inspección física del contenedor por la Aduana del Gobierno anfitrión, actuando CBP como observadores;
¬ Aquellos contenedores de bajo riesgo, o los que han sufrido una pre-inspección o inspección física con resultado satisfactorio pueden entrar en los Estados Unidos sin demoras.
Con estas medidas se pretende un incremento de la seguridad sin suponer restricciones al comercio legal.

C.S.I. en España
En el momento de lanzamiento de la iniciativa, únicamente el Puerto de Algeciras estaba incluido entre los que podían participar en C.S.I., lo que sin duda significaba una desventaja para los

the American Customs for the country to be selected as a C.S.I. participant are:
¬ The Customs Administration in the host country must be able to inspect the containers whose cargos originate in that country, or have been transferred to that country or are in transit in that country;
¬ The selected port or ports must have considerable regular and direct traffic with the United States;
¬ An undertaking must be given to establish an automated system for analysing risks in order to identify potentially dangerous containers;
¬ An undertaking must be given to share information, vital data and risk management with US CBP and to develop a procedure for making it easy to exchange such information;
¬ The port facilities and infrastructures must be subjected to a risk analysis process and an undertaking must be given to make improvements where weaknesses exist.
As has already been explained, one of the points on which the operability of the system is based, is the availability of non-intrusive inspection equipment for containers. With a view to complying with this requirement the Port Authorities for the Bay of Algeciras, Barcelona and Valencia have recently contracted the purchase of three non-intrusive mobile inspection systems, which use X-rays to obtain an image of the inside of the containers. These items of equipment are mounted on a lorry and will be operational in approximately two months.

Modifications to the SOLAS Agreement. ISPS/ISPS Code

Furthermore, as a consequence of the events of September 11th 2001, in its meeting held in November of that same year, the International Maritime Organisation agreed to prepare measures to improve the protection of vessels and ports, which were subjected for approval to the Diplomatic Conference on Maritime Protection.
This Conference was held in London in December of the following year, 2002, was prepared by the IMO Maritime Security Committee (MSC), and gave its approval to additional provisions to the SOLAS agreement as well as implementing the ISPS Code.

Puertos de Barcelona y Valencia, igualmente con tráficos importantes hacia los Estados Unidos. Es por ello que el acuerdo firmado entre CBP y la Aduana de España incluía a los tres puertos en el programa.
Los requisitos que exige la Aduana americana para que un país sea seleccionado como participante en C.S.I. son:
¬ La Administración de Aduanas del país anfitrión debe tener la capacidad de inspeccionar los contenedores cuya carga sea originada, transbordada o se encuentre en tránsito en ese país;
¬ El puerto o los puertos seleccionados deben tener un tráfico significativo, regular y directo con los Estados Unidos;
¬ Se debe comprometer a establecer un sistema automatizado de análisis de riesgos para identificar los contenedores potencialmente peligrosos;
¬ Debe comprometerse a compartir información, datos críticos y gestión de riesgos con US CBP y desarrollar un procedimiento para facilitar estos intercambios;
¬ Debe realizar una evaluación de riesgos de las infraestructuras del puerto y comprometerse a mejorar sus vulnerabilidades.
Como se ha explicado, uno de los puntos en los que se basa la operatividad del sistema es la disponibilidad de equipos de inspección no intrusiva de contenedores. Para cumplir este requisito, las Autoridades Portuarias de Bahía de Algeciras, Barcelona y Valencia han contratado recientemente la adquisición de tres sistemas móviles de inspección no intrusiva, que utilizan los rayos X para la obtención de una imagen del interior de los contenedores. Estos equipos van montados sobre camión y serán operativos en dos meses aproximadamente.

Modificaciones al Convenio SOLAS. Código PBIP/ISPS

Igualmente como consecuencia de los acontecimientos del 11 de Septiembre de 2001, la Asamblea de la Organización Marítima Internacional, en su sesión de Noviembre de ese mismo año acordó la elaboración de medidas para mejorar la protección de buques y puertos, que se someterían a su aprobación en una Conferencia diplomática sobre protección marítima.
Esta Conferencia se celebró en Londres en Diciembre del siguiente año, 2002, fue preparada por el Comité de Seguridad Marítima de IMO, MSC, y aprobó nuevas disposiciones del Convenio Solas y la implantación del Código de Protección de Buques e Instalaciones Portuarias, o Código PBIP.
Las medidas adoptadas en la Conferencia de Londres incluyen:
¬ Modificaciones al Capítulo V del SOLAS, Convenio para la Seguridad de la Vida Humana en el Mar, en el que se fija un calendario acelerado para la instalación de un sistema automático de identificación AIS, que deberá estar en operación en todo momento excepto cuando sea decidido por acuerdos internacionales;
¬ Se modifica el Capítulo XI, relativo a medidas especiales para la mejora de la seguridad marítima, que pasa a denominarse XI-1. Estas modificaciones incluyen la obligación de que los buques lleven permanentemente marcado el número de identificación, en el casco o en la superestructura, y en los buques de pasaje estará dispuesto en un plano horizontal para que sea visible desde el aire;
¬ También en el Capítulo XI-1 se añade un nuevo requerimiento, el relativo al mantenimiento de un registro sinóptico continuo, CSR de la historia del buque, que debe contener la principal información sobre el buque, como su nombre, bandera, puerto de registro, el número de identificación o el nombre y la dirección del propietario;
¬ Finalmente se añade el Capítulo XI-2, que incluye el Código PBIP;
¬ En este Capítulo, también se incluye la obligación de equipar a los buques con un sistema de alerta, SSAS, que sea capaz de transmi-

The measures adopted at the London Conference include the following:
¬ Modifications were made to Chapter V of SOLAS, Agreement for the Security of Human Life at Sea, in which a speeded up schedule was established for installing an Automatic Identification System (AIS), which must be operating at all times except when a decision to the contrary is reached by international agreement;
¬ Modifications were made to Chapter XI, concerning special measures for improving maritime security, which came to be known as XI-1. These modifications include the requirement that ships bear their identification number indelibly marked on the hull or the superstructure, and that passenger ships have this number laid out horizontally on deck, so that it is visible from the air;
¬ A further provision is also added to Chapter XI-1, requiring vessels to keep a synoptic log concerning the keeping of a Continuous Synoptic Register (CSR) of the history of the ship, which must contain all the important information about the vessel, such as its name, flag, the port where it was registered, the identification number or the name and address of the owner;
¬ Finally, Chapter XI-2 is added, which includes the ISPS Code;
¬ The above Chapter also includes the requirement to equip vessels with an alert system, SSAS that can transmit a vessel-land alarm to the appointed authority containing information that identifies the ship, its position and indicating that the vessel's security is jeopardised. It must not be possible to detect the alarm from the vessel itself, and it must be possible to give the alarm from two different points, one of which has to be the bridge.
As it is a subject for more detailed explanation, it can be said that the ISPS Code is applied to passenger ships, with a tonnage equivalent to or greater than 500 GT, to mobile drilling units and to port facilities that provide service to these vessels and devices, as long as they are involved in international traffic movements.
The Code makes Port Facility Protection Assessment compulsory, and also makes it necessary for a Facility Protection Plan to be prepared and approved and for a PI protection officer to be appointed. Three protection levels are considered, Level 1, ongoing measures, Level 2, further temporary measures owing to an increase in risk and Level 3, specific temporary measures due to the possibility or imminence of an event.

Regulation 725-2004
In April 2004 EC Regulation 725/2004 was published by the European Parliament and Council, concerning improvements to the protection of ships and port facilities, which applies the measures contained in the ISPS Code with certain differences.
It defines the main objective of implementing and applying measures that improve protection for ships involved in both international and domestic traffic, and the port facilities associated with them. This marks an essential difference with respect to the ISPS Code.
It also aims to be a tool used for interpreting and applying the special measures to be implemented to increase maritime protection to which approval was given by the Diplomatic Conference of the IMO in December 2002, referred to above.
The Regulations establish their sphere of application as follows:
¬ 1st July 2004, the special measures are applied to increase maritime security as established by SOLAS to the vessels envisaged by virtue of this Agreement;
¬ 1st July 2005, those measures are applied to Class A passenger ships in domestic traffic and the terminals at which they operate;
¬ 1st July 2007 to the rest of the ships and terminals, to the extent that this is decided upon by the Member States.

Directive 65/2005
Finally, European Parliament and Council Directive 65/2005 was published in November 2005 concerning protection for port improvements.
This Directive extends these measures that applied to port facilities, as envisaged in Regulation 725/2004, so that they now apply to the whole port, within the limits defined by each Member State, with a view to ensuring that the measures envisaged in that Regulation received greater protection.
This standard shall be enforced no later than June 15th 2007.

tir una alarma buque-tierra a la autoridad designada con información de la identificación del buque, su posición y la indicación de que la seguridad del buque está en peligro. La alarma no debe ser perceptible desde el mismo buque, y debe poder ser activada desde dos puntos diferentes, uno de ellos el puente de navegación.
Por ser tema de una más precisa exposición, diremos que el Código PBIP se aplica a los buques de pasaje, a los de arqueo igual o superior a 500 GT, a las unidades móviles de perforación y a las instalaciones portuarias que den servicio a estos buques y artefactos, siempre que efectúen tráfico internacional.
El Código obliga a la realización de una Evaluación de la Protección de la Instalación Portuaria, a la realización y aprobación de un Plan de Protección de la Instalación y al nombramiento de un Oficial de Protección de la IP. Se consideran tres niveles de protección, el Nivel 1, de medidas permanentes, el nivel 2, de medidas adicionales temporales por aumento de riesgo y el nivel 3 de medidas concretas temporales por posibilidad o inminencia de un suceso.

El Reglamento 725-2004
En Abril de 2004 se publica el Reglamento (CE) 725/2004 del Parlamento Europeo y del Consejo relativo a la mejora de la protección de los buques y las instalaciones portuarias, que aplica las medidas del Código PBIP con algunas diferencias.
Define su objetivo principal el de instaurar y aplicar medidas que mejoren la protección de los buques utilizados tanto en el tráfico internacional como nacional, y de las instalaciones portuarias asociadas a los mismos. Esta es una diferencia fundamental con el Código PBIP.
Además pretende ser un instrumento para una interpretación y aplicación armonizada de las Medidas especiales para incrementar la protección marítima aprobadas por la Conferencia Diplomática de OMI de Diciembre de 2002, ya comentadas con anterioridad.
El Reglamento establece su ámbito de aplicación como sigue:
¬ El 1 de Julio de 2004, se aplican las medidas especiales para incrementar la seguridad marítima de SOLAS a los buques previstos en ese Convenio;
¬ El 1 de Julio de 2005, se aplican esas medidas a los buques de pasaje pertenecientes a la clase A en tráficos nacionales y a las terminales en las que operan;
¬ El 1 de Julio de 2007 al resto de los buques y terminales, en la medida en que decidan los Estados miembros.

Directiva 65/2005
Finalmente, en Noviembre de 2005 se ha publicado la Directiva 65/2005 del Parlamento Europeo y del Consejo sobre protección de la mejora portuaria.
Esta Directiva amplía las medidas que, para las instalaciones portuarias, preveía el Reglamento 725/2004, a la totalidad del puerto, dentro de los límites definidos por cada Estado miembro, con el objeto de que las medidas previstas en dicho Reglamento se beneficien de una mayor protección.
Se debe dar cumplimiento a esta norma no más tarde del 15 de Junio de 2007.