OCDE

OECD

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY

SECURITY IN MARTIME TRANSPORT: RISK FACTORS AND ECONOMIC IMPACT

Maritime Transport Committee

July 2003

This report explores the risks posed to the international merchant maritime transport system by terrorist organisations. As a part of this vulnerability analysis, the paper explores the possible economic repercussions of a terrorist attack involving maritime transport. The second part of the paper explores the cost implications of security measures enacted in response to this threat.

Organisation for Economic Co-operation and Development
Organisation de Coopération et de Développement Economiques

EXECUTIVE SUMMARY

1. Immediately after the devastating September 11th World Trade Center attacks in New York, governments around the world scrambled to assess their vulnerability to highly organised terrorist groups willing to sacrifice thousands of lives to achieve their aims. The risk of mega-terrorism, once the stuff of spy novels, suddenly became very real, and the maritime transport system loomed large in the eyes of security agencies worldwide as a prime target and/or vehicle for future attacks.

2. World trade is dependent on maritime transport and great strides have been made in recent years to render this system as open and frictionless as possible in order to spur even greater economic growth. However, the very things that have allowed maritime transport to contribute to economic prosperity also render it uniquely vulnerable to exploitation by terrorist groups. The risks are numerous and encompass both containerised and bulk shipping. The vulnerabilities are important, and range from the possibility for physical breaches in the integrity of shipments and vessels to documentary fraud and illicit money-raising for terrorist groups. Finally, the stakes are extremely high, as any important breakdown in the maritime transport system would fundamentally cripple the world economy.

3. Against this backdrop, governments have set in place a series of actions aimed at reducing the risk from the most obvious security gaps in the maritime transport network. The bulk of these have been negotiated at the International Maritime Organization and are set to become effective in July 2004. Additionally, the United States has also developed a set of maritime security measures that are comprised of both mandatory and voluntary elements.

4. These measures come at a cost which this report has tried to ascertain at a very early stage in their implementation – most measures were not yet in place at the time of writing and those that were had only just been implemented. Nonetheless, three broad conclusions emerged from this overview.

5. The first is that the costs of inaction are potentially tremendous. The maritime transport system *is* vulnerable to being targeted and/or exploited by terrorists. A large attack, especially a well-co-ordinated one, could have the result of shutting down the entire system as governments scramble to put in place appropriate security measures. These may be drastic, such as the complete closure of ports, and inefficient, such as duplicative and lengthy cargo checks in both originating and receiving ports. The cost of such an attack would likely be measured in the tens of billions of dollars (*e.g.* up to USD 58 billion for the United States *alone*). It is precisely for these reasons that governments have sought to strengthen their security dispositions *vis-à-vis* maritime transport.

6. The second is that some costs are more easily measured than others – and that those costs that can be measured with some precision are significantly less than the potential cost of doing nothing. Generally, ship-related costs tend to be relatively easy to ascertain as these involve specific equipment purchases and labour costs at known international rates. We estimate the initial burden on ship operators to be *at least* ~USD 1 279 million and USD 730 million per year thereafter. The bulk of ship-related costs are related to management staff and security-related equipment expenditures. . Estimates on port-related security costs are extremely difficult to derive as it is yet uncertain what the impact of IMO measures will be on a hiring of new security personnel and if so, what will be the applicable labour rates. Some of the most difficult costs to estimate are those that derive from system-wide procedural changes such as those imposed by the

United States 24-hour advance notice rule. However, even in the later case, the estimate of approximately USD 281.7 million (using carriers' data) is still significantly below the potential costs of inaction. Overall, we find that, for those costs that can be measured, the resulting figure of slightly over USD 2 billion is still substantially below the costs that might result from a major attack.

7. Finally, the focus of this report has been on *costs*, it should be pointed out, however, that many of the measures proposed have distinct *benefits* that are not related to their anti-terrorism task. These benefits result from reduced delays, faster processing times, better asset control, decreased payroll (due to IT improvements), fewer losses due to theft, decreased insurance costs, etc. These savings can be significant, and can serve to counter-balance the increase in security costs.

8. While the calculation of these benefits falls beyond the scope of this report, some insight may be gained by looking at non-security inspired projects that may have similar impacts on trade facilitation. For example, cost-benefit analyses of a new electronic customs manifest handling system proposed by American Customs before September 11th, 2001, estimate the direct savings to American importers alone to be USD 22.2 billion over 20 years and the American government savings to be USD 4.4 billion over the same period. While these estimates are not directly transposable to security-related measures, they do provide a glimpse of the type of savings that can be realised as a result of faster processing times, better asset control, reduced theft, etc. – all potential benefits of the new maritime security measures.

9. In the end, most participants in the international maritime trading system agree that the recently enacted maritime security measures are desirable. They are not free, but they do bring about benefits that go beyond their mitigating impacts on terrorism. The extent of their costs is uncertain but it is likely to be much less than the extent of costs linked to inaction. What is certain is that some of these measures have the potential to change long-established practices in the industry – for the better.

1. INTRODUCTION

10. Freely flowing international trade, carried predominantly by a large and heterogeneous fleet of ocean-going vessels, has been the impetus behind the significant advances in world prosperity experienced in the second-half of the 20th century. Decreased trading barriers and reduced tariffs have facilitated the development of a truly interlinked and globalised economy. The business community has responded to this new trading environment and has increasingly sought commercial partners, suppliers and customers throughout the globe. The very act of producing goods for markets has also changed radically as suppliers and manufacturers have developed efficient production processes that reduce inventory-holding to a very minimum – production processes made possible by fast, efficient and unfettered international transport. The emerging paradigm for global prosperity has been predicated on near-frictionless transport and trade.

11. This paradigm changed, however, in one horrible day.

12. The initial reactions to the extraordinary 11 September 2001 attacks on the New York World Trade Center Towers by Al'Qaeda operatives focused on the air transportation system. For the first time in its history, the United States completely closed down its airspace to commercial aviation. This measure was understandable given that commercial jets had served as the vector for these attacks. While still a focus of heightened security, the maritime sector remained relatively untouched at the time. Despite the temporary closure of regional ports in the New York area and the interdiction of certain ships in the immediate aftermath of the attacks, trade still flowed freely and the masses of containers and bulk commodities that fuel the world economy continued to flow unimpeded.

13. However, as the level of sophistication, organisation and financing involved in the Al'Qaeda attacks became apparent, governments quickly intensified their scrutiny of the maritime sector, and for good reason. Here is a sector characterised by an extremely diverse international labour force, transporting a vast range of goods whose provenance, description and ownership are often left remarkably vague. This is a system where international transport chains involved thousands of intermediaries, on vessels registered in dozens of countries that sometimes choose not to uphold their international responsibilities and where some vessel owners can and do easily hide their true identities using a complex web of international corporate registration practices. Furthermore, this system had already displayed certain vulnerabilities in the past, especially with respect to its use for the illegal smuggling of drugs or banned goods. And yet this system remains absolutely essential for continued world trade and prosperity. For all of these reasons, the international transport of goods by sea quickly moved to the fore of the international agenda to combat terrorism.

14. No one has seriously proposed that the maritime trading system should be closed down through draconian security measures, and the world community still strongly believes that the twin objectives of trade facilitation and transport efficiency remain as valid now as before 11 September 2001. However it has become evident that these twin objectives must be balanced with heightened security measures that address the system's vulnerabilities and weaknesses. The bulk of the new maritime security measures have emerged from two fora. The first raft of measures emerged in December of 2002 from negotiations at the International Maritime Organization in the form of the International Ship and Port Safety (ISPS) Code. This code enacts changes to the Convention on the Safety of Life at Sea (SOLAS). The second set of measures are largely supplementary to the ISPS and have been developed and adopted by the government of the United States in response to its own analysis of the vulnerabilities of the maritime transport system.

15. This report explores the risks posed to the international merchant maritime transport system by terrorist organisations[1]. As a part of this vulnerability analysis, the paper explores the possible economic repercussions of a terrorist attack involving maritime transport. The second part of the paper explores the cost implications of security measures enacted in response to this threat.

16. At the time of this report's writing, the world had thankfully not experienced a major terrorist attack using ships or maritime infrastructure. The cost estimates of such an event provided in this report therefore should only be taken as an approximation. While these are based on a broad range of sources and can be considered to be a reasonable estimation, they are only indicative of the magnitude of costs. Likewise, at the time of writing, many international and/or national maritime security measures were only just in the process of being implemented. Given the lack of actual experience with the new measures, estimates of the costs of these range from fairly precise (when these account for mandated equipment costs) to necessarily vague (*e.g*. when system-wide procedural changes are under consideration). Again, these estimates should serve as an indication of the *magnitude* of likely costs, rather than *exact* costs, imposed by maritime security measures.

[1] Security costs for passenger vessels, while important, fall beyond the scope of this report.

2. RISK FACTORS: WHAT ARE THE THREATS?

17. Perhaps foremost among the risk factors associated with maritime transport is the sheer volume and numbers of goods moving by sea. The United Nations Conference on Trade and Development (UNCTAD) estimates that 5.8 billion tons of goods were traded by sea at in 2001. This accounts for over 80% of world trade by volume. The bulk of this trade is carried by over 46 000 vessels servicing nearly 4 000 ports throughout the world. And there are no signs that world maritime trade will be decreasing any time soon, especially as international negotiations have expressly sought to facilitate and accelerate world trade rather than slow it down.

18. In addition to its size, the maritime sector, by its very nature as a complex, international open transportation network, poses several additional challenges from a security standpoint. One of these is the multiplicity of terrorist risk factors associated with shipping.

19. Sea-going vessels can be the vector for, or target of, attacks. They can also serve to facilitate other attacks and/or raise revenue for terrorist organisations. The principal risk factors related to shipping – cargo, vessels, people and financing – are also linked to the broader risk of major disruptions in world trade and increased economic costs linked to heightened security. It is important that governments address all of these risks with broad-based security policy responses, since simply responding to threats in isolation to one another can be both ineffective and costly.

Risk factors: cargo

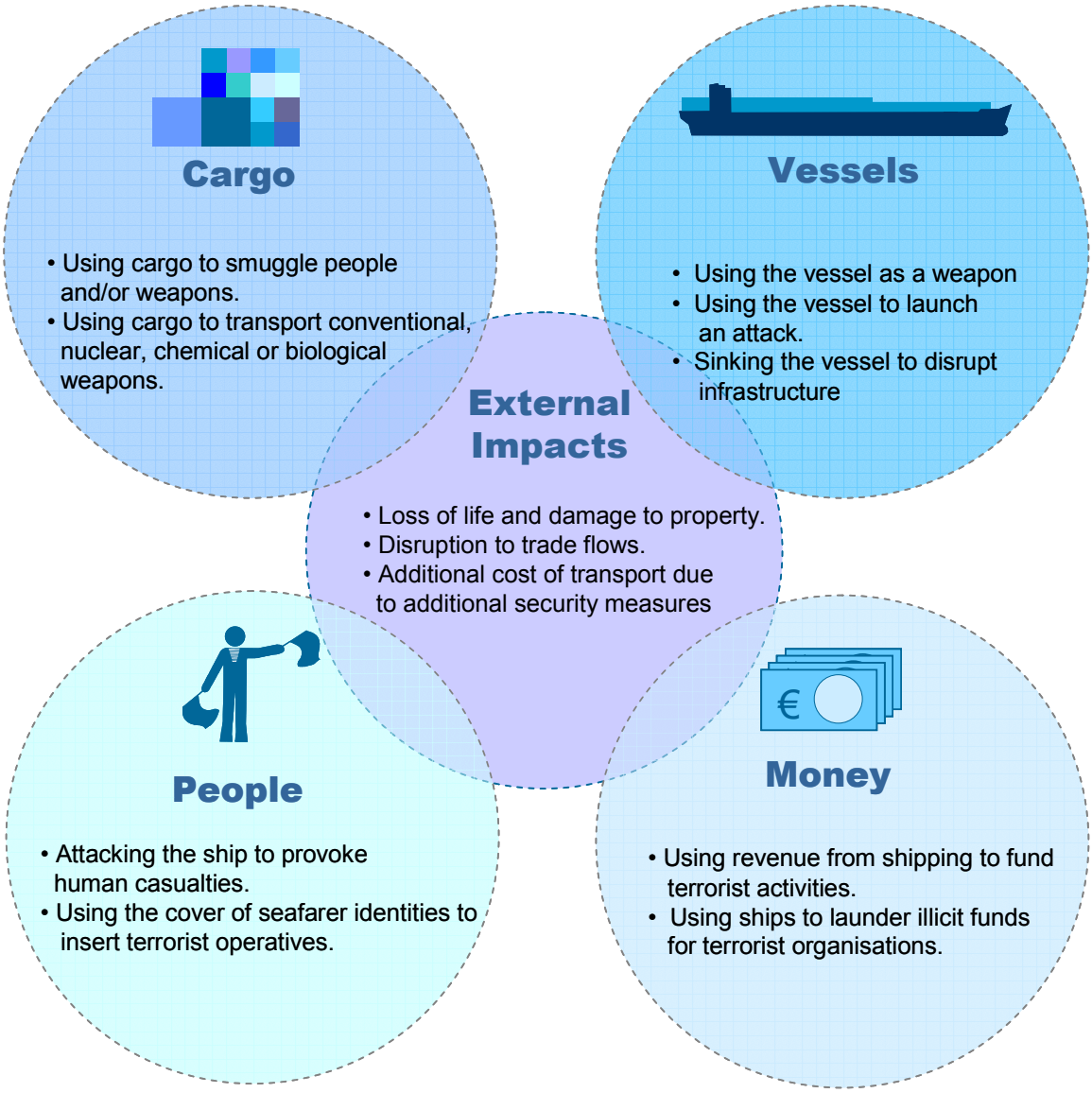
Containers

20. Most of the world's non-bulk cargo travels in marine shipping containers. These standardised boxes have revolutionised the transport of goods by sea since their first appearance in the 1950's and have given rise to a multitude of specialised road and rail carriers, a fleet of over 2 700 modular container vessels and the emergence of a global network of over 430 highly automated port handling facilities. In 2002, the Bureau International des Containers (BIC) estimated that approximately 15 000 000 containers were in circulation – almost evenly shared between the self-owned and leased fleet. Data from Containerisation Online indicate that 232 million containers were moved through container ports in 2001. The staggering volume of container movements, their relatively high velocity in the international trading system and their uniformity all pose formidable challenges from a security perspective.

21. The first of these is that the system is porous enough that it can be relatively easily subverted from legitimate commercial purposes. Section 4 provides a brief description of the container transport chain and highlights many of the system's current vulnerabilities. Suffice to say that the opportunities are numerous to misuse this mode of freight shipment.

22. Immediately following the World Trade Center attacks, attention quickly shifted to the possibility that containers could be used to conceal and deliver relatively crude weapons of mass destruction. In a worst case scenario, a terrorist organisation could pack a global positioning satellite-enabled weapon of mass destruction within a shipping container, introduce it into the international transport system using legitimate shippers, intermediaries and carriers, and remotely detonate the weapon upon its arrival in the

heart of a major population centre. All that would be required is a weapon, a few well-placed agents and a basic understanding of international trading practices. The likelihood of success of such an operation would be heightened by that fact that only a small number of containers are ever physically examined (*e.g.* approximately 2% in the United States prior to the World Trade Center attacks).



23. The fear that terrorists could exploit the container transport system for their ends was confirmed on 18 October 2001 when port authorities in the southern Italian port of Gioia Tauro discovered a stowaway within a well-appointed shipping container complete with bed, heater, toilet facilities and water. The man's belongings included a cell phone, a satellite phone, a lap-top computer and, ominously, given recent events, airport security passes and an airline mechanic's certificate valid for New York's JFK, Newark, L.A. International and O'Hare airports. After his arraignment and subsequent release under bond, the stowaway disappeared before further information could be gathered. However, what did become apparent was the apparent ease with which the container transport system was subverted in this case. The

container slot was chartered by Maersk Sealand's Egyptian office and the container loaded in Port Said onto the German-owned, Andrew Weir-chartered, Antigua & Barbuda flagged, 2 959 TEU Ipex Emperor. The container was set to be transhipped at Gioia Tauro, carried to Rotterdam before once again being transhipped to its final destination in Canada. With the exception of its unusual cargo, this container move was nearly indistinguishable from any of the other 2.5 million handled at Gioia Tauro in 2001. In fact, had the stowaway not been attempting to widen the container's ventilation holes when port workers were nearby, the container would have likely passed through unhindered to its final destination.

24. Long before the world focused its attention on the possibility for terrorists to use containers as delivery vehicles for weapons of mass destruction and/or operatives, customs authorities had already been fighting a rear-guard battle against the misuse of containers by drug dealers, crime syndicates and contraband traders.

25. Figures on the amount of drugs and illegal goods concealed within containers are hard to come by – but what is certain is that the system has been, and continues to be, exploited by clever criminals. Authorities in the United States, one of the world's leading destination for illegal drugs, reported 950 seizures of cocaine, marijuana and heroin in commercial ocean cargo shipments and vessels from 1996 to 1998 – accounting for 223 502 kilos of drugs. When these figures are compared to the other main drug entry pathway into the United States – along the Southwest land border with Mexico – it becomes apparent that the maritime vector seems to be the preferred option for drug smugglers. Seizures in 12 seaports surveyed by the United States Interagency Commission on Crime and Security in American Seaports accounted for 69%, 55%, and 12% respectively for all cocaine, marijuana and heroin seized nationwide (by weight). Analogous figures for the Southwest American border were 13%, 36% and less than 1%, respectively. A substantial proportion of drugs seized in American seaports was found concealed in shipping containers.

26. Beyond their criminal uses for drug and contraband goods smuggling, containers have also been the target of cargo thieves' intent on quickly and easily stealing high-value cargoes. Estimated losses from cargo theft range from USD 30 to USD 50 billion per year – with most of the thefts involving trucks. However, seaports and container staging areas are also prone to containerised cargo theft. Port container crime is often accompanied by some form of internal conspiracy where criminals are assisted by individuals legitimately employed in seaports or in the transport industry. These conspiracies enable thieves to correctly identify and target containers carrying high-value goods. The level of sophistication involved in some cases of cargo theft is such that sealed containers can be rapidly emptied with no exterior signs of foul play. The same techniques employed by thieves – use of a network of conspirators and technical means to bypass container doors, seals and locks – can be also used by terrorists intent in placing a load within the container and/or removing a shipment sent by colleagues overseas.

27. Containers also pose a threat when they carry legitimate cargo that can be used by terrorists for nefarious purposes. Many containers and/or tank-containers are used to ship hazardous cargo. These cargoes are diverse and can include explosive compounds, munitions, fireworks and dangerous chemicals. While thousands of hazardous goods containers are safely shipped every day, several significant accidents have occurred in the past. For example, in November 2002, an explosion involving improperly stored fireworks and calcium hypochorite containers (a bleaching agent used in swimming pools) caused one death and extensive damage to the 4389 TEU *Hanjin Pennsylvania* and its' cargo near Sri Lanka. Other explosions and fires linked to containers carrying calcium hypochorite include the *Sea-Land Mariner* near Crete in April, 1998 and the *CMA Djakarta* near Egypt in July 1999.

28. In another example of the risk posed by certain containerised cargoes, storm damage to the *Santa Clara I* off the eastern coast of the United States in January 1992 caused several containers containing magnesium phosphide to spill their contents in the hold. This compound, when mixed with air and/or water

forms two highly reactive gases – phosphene and diphosphane – that can explosively auto-ignite at ambient temperatures. Cargo loss surveyors did not realise the danger posed by the spill in Baltimore, the ship's first port of call, and it was only on survey in the following port, Charleston, that the danger was recognised. In this case, danger was averted by quick decontamination and clean-up but had the gas ignited, the force of the resulting explosion would likely have caused significant damage to the port area and surrounding neighbourhood.

Risks of hazardous goods containers: internal hold of the Hanjin Pennsylvania, November 2002

Source: photo credit: Countryman & McDaniel (www.cargolaw.com).

29. In the case of the *Santa Clara I*, the magnesium phosphide containers were improperly manifested thus hiding the dangerous nature of their contents. This case of mislabelled containers is not a unique occurrence and, because of the constraints placed on hazardous compound handling and stowage both in ports and on ships, some unscrupulous shippers and forwarders ambiguously- and/or mis-label containers containing these compounds. Anecdotal evidence from the port of Rotterdam provides an indication of the extent of the phenomenon as recent container inspections have revealed that a significant number of containers containing Class 1.1 fireworks (according to the International Maritime Organization's International Maritime Dangerous Goods – IMDG – Code) were mislabelled as less dangerous Class 1.3 and 1.4 fireworks – presumably to avoid the constraints, permitting costs and delays imposed on the import of Class 1.1 substances.

30. The fact that some unscrupulous shippers and/or careless carriers sometimes mask the true identity of hazardous cargo underscores the ease with which terrorists could do the same for more sinister purposes. Terrorists could use knowledge of legitimate hazardous cargo and/or conceal the true identity of otherwise dangerous goods in order to place such containers onboard vessels where they can then be detonated, provoking damage ranging from the loss of a substantial part of the cargo to destruction of port infrastructure and its surroundings.

Bulk shipments

31. The other principal maritime freight sector – bulk shipping – has generally received less scrutiny from security authorities. This sector is divided between bulk liquid shipments (ranging from crude oil, distilled oil derivatives, LPG and LNG to molasses and vegetable oils) and solid bulk cargoes. The risk posed by liquid bulk cargoes is commensurate with their volatility with some cargoes presenting extreme risks (gasoline, kerosene, LPG and LNG). Security efforts targeting bulk shipments have focused most on shipments of volatile liquid compounds -- *e.g.* one of the first maritime related security actions taken following the World Trade Center attacks was to ban entry to a shipment of LNG to Baltimore harbour on 12 September 2001.

32. Shipments of LPG and LNG have generated special concern among security agencies and have prompted special navigational restrictions and escort requirements in many ports for the world's fleet of approximately 1 153 LPG/LNG tankers. While the destructive potential of these cargos is great, it must be noted that LPG/LNG tankers tend to be expensive and relatively modern vessels operated by reputable firms. Furthermore, given the dangerous nature of their cargoes, these vessels tend to have robust cargo security systems in place (*e.g.* a November 2002 fire aboard the LPG tanker *Gaz Poem* failed to ignite the partially laden tanks. In another example, a direct hit on a LNG cargo tank by an Exocet missile during the Iran-Iraq war also failed to cause an explosion). The principal risk from these types of cargoes is posed during loading and/or unloading operations when the cargo can accidentally be released in a gaseous state. These factors make it relatively unlikely that a terrorist group could successfully rig the explosion of a LPG/LNG vessel's cargo. To a lesser extent, terrorist groups would face similar difficulties in seeking to detonate other volatile liquid cargos. In any case, there are many easier targets in bulk shipping for terrorists to choose from – such as the bulk shipping sector.

33. While the majority of bulk shipments carried by the world's fleet of 23 281 bulk/general cargo vessels carries relatively inert compounds such as iron ore, coal, grains, bauxite/alumina and rock phosphate, a certain number of bulk cargoes are considered extremely hazardous and have the potential to be manipulated by organised terrorists groups. Chief among these are bulk shipments of fertilizers such as ammonium nitrate.

34. Ammonium nitrate is widely used throughout the world as an agricultural fertilizer and is generally considered a safe and stable compound when stored and handled correctly. However, with some manipulation (*e.g.* through the addition of fuel oil) and triggered by a sufficiently large explosive catalyst, fertilizer grade ammonium nitrate can be used as a powerful explosive. Terrorist organisations throughout the world have been known to use adulterated nitrogen fertilizers to make powerful explosives (*e.g.* the truck bombings in Bali, Nairobi, Mombassa, Oklahoma City as well the first World Trade Centre attack) prompting many countries to ban the import of ammonium nitrate. The scale of potential destruction by a shipload of ammonium nitrate is several orders of magnitude greater than these truck bombs as can be seen from the 1947 Texas City explosion or the recent massive ammonium nitrate explosion in AZF plant in Toulouse, France.

35. OECD countries imported over 1.6 million tons of ammonium nitrate in 2000 – mostly by sea. Bulk shipments of nitrogen fertilizers receive greater scrutiny and are typically handled in accordance with the IMO Code of Safe Practice for Solid Bulk Cargoes. However, this code is designed to reduce the risk of *accidents* involving hazardous compounds such as ammonium nitrate – as such, it does not guarantee that such shipments might not be wilfully rigged and detonated by determined terrorists. The configuration of many fertilizer importing/exporting ports further contributes to making these shipments a prime terrorist target. For example, in 1997, over 400 000 tonnes of ammonium nitrate were shipped along the winding 235-mile-long lower Mississippi waterway, the world's largest bulk commodity port area. Many of these shipments pass by the populous city of New Orleans on their way to ports upstream, heightening the

potential impact from a terrorist explosion. Similarly, the port of Rotterdam also receives a significant amount of fertiliser traffic along its narrow access channel where the risk to other port infrastructure is elevated.

36. Another risk to be considered in the shipment of dry bulk cargoes is the general structure of the tramp freighter fleet. A significant number of these vessels are operated as one vessel companies using opaque ownership mechanisms. The fleet is generally older (*e.g.* 78% of the bulk/general cargo fleet is over 10 years old vs. 66% for LNG/LPG carriers and 73% for the world commercial fleet in 2001 – Lloyd's List World Flet Statistics) and is characterised by a larger percentage of sub-standard – and therefore presumably less scrupulous owners. Past efforts aimed at reducing the incidence of sub-standard shipping have revealed the difficulty of positively identifying these owners. Organised terrorist groups have in the past used commercial vessels to support their operations and it is likely that they will continue to do so (see discussion on page 14). Reports from United States intelligence sources indicate that the Al'Qaeda group is suspected of owning or having long-term time-charters on a fleet of 15-18 bulk/general cargo vessels[2]. While it is believed that these vessels are used to generate revenue and/or support the group's logistics network, it is feasible that one of these vessels could be used in a "suicide" operation making use of a modified fertiliser cargo.

Risk factors: vessels

37. The previous section discusses the dangers posed by bulk vessel cargoes. These dangers highlight the potential for an entire vessel to be used as a weapon in a terrorist strike just as jet aircraft were used in the 2001 World Trade Center attacks. In such cases, a vessel can be used against a population centre adjacent to port facilities and/or shipping channels, to damage port facilities themselves or to sink the vessel(s) and block access to a port facility.

38. While the potential damage from such an attack is great, previous terrorist incidents involving ships have tended to *target* vessels rather than use them. The boarding of the cruise vessel *Achille Lauro*, the suicide attacks against the *USS Cole* and the oil tanker *Limberg,* and the discovery of an Al'Qaeda linked plot to attack vessels passing through the straits of Gibraltar, all point to the risk of attack faced by vessels. Given the relative difficulty in triggering a major explosion through an attack on a vessel, it is more likely that the principal motivation for terrorists to attack a vessel would be to hijack its cargo, hold its crew hostage for ransom or political purposes, sink the vessel and cause as much loss of life as possible, or cripple trade by threatening to close down access to ports and/or vulnerable trade routes.

39. The risk to shipping from terrorist attacks is underscored by the persistent problem of modern-day piracy. Every year cargo, passenger and fishing vessels come under attack by pirates seeking to gain revenue by hijacking and selling cargo and/or ransoming crew. While most incidents involve attacks and thefts from vessels at anchor or in ports, a significant number of attacks are mounted by relatively well organised and heavily armed gangs of pirates on the high seas. In the years 1999-2001, the Piracy Reporting Centre of the International Chamber of Commerce registered a record number of attacks against vessels. Targets of these attacks included most classes of vessels: bulk/general cargo vessels, tankers, container carriers and chemical and LPG carriers. The attacks were concentrated in several distinct geographical areas including the Malacca straits, Indonesian and Malaysian waters, the coasts of Bangladesh and India, the Red Sea/Horn of Africa area and the west coast of Africa.

---

[2] "15 Freighters Believed to Be Linked To Al Qaeda", *Washington Post*, December 31, 2002.

Acts of piracy: 1999-2001

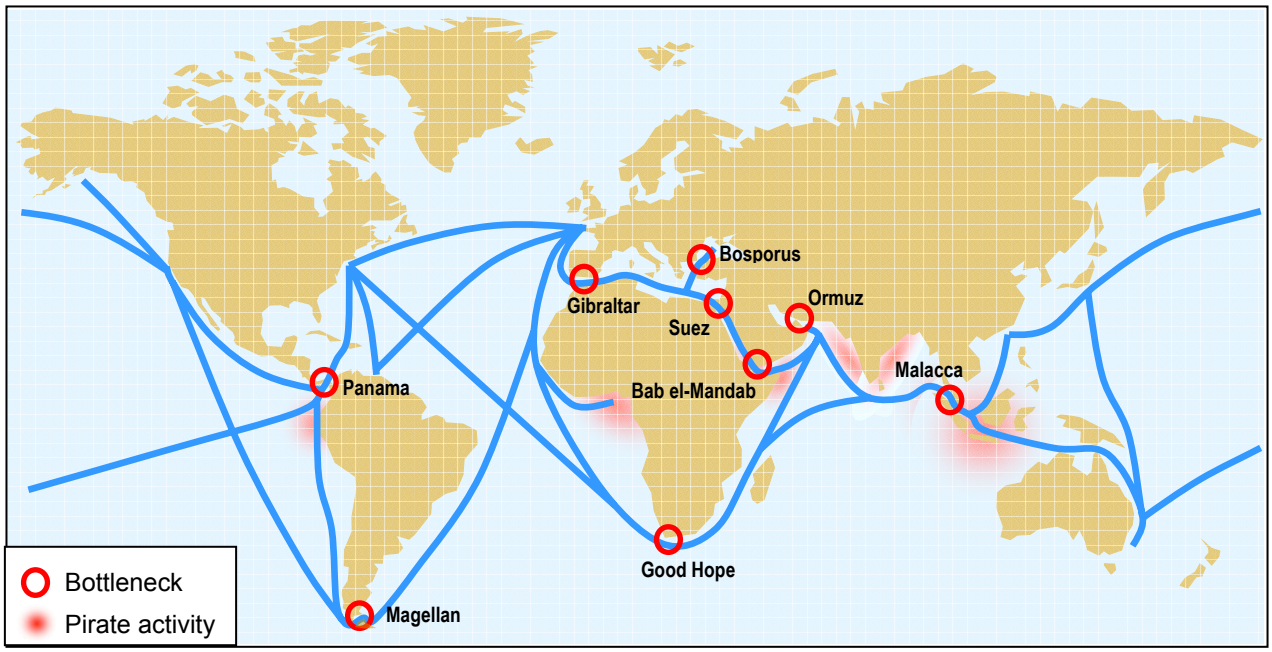
Vessel attacked while…	1999	2000	2001
Underway	103	146	130
At anchor	144	210	156
At berth	25	50	46
Unspecified	13	63	2
Total	**285**	**469**	**335**

Source: Source International Chamber of Commerce (ICC) International Maritime Bureau, Piracy Reporting Center.

40. Piracy can be a highly lucrative venture considering that many vessels carry large sums of cash in order to pay for port fees and crew salaries. Crew members can also be ransomed for cash. In some cases, however, pirates hijack the entire vessel and sell the cargo for considerable profit (*e.g.* up to USD 1 000 000 in the case of an oil tanker). Furthermore, a hijacked vessel can be turned into a source of steady revenue by being operated as a "ghost" vessel. In this instance, the hijacked ship is re-painted, renamed, supplied with false documentation and operated as a commercial vessel. Unsuspecting and time-pressed shippers contract for carriage of their goods on the "ghost" vessel through a normal commercial transaction. Once underway, however, the ship is diverted, the cargo sold and the cycle repeats itself in another port.

41. Organised, sophisticated and cash-flush criminal gangs are active in south-east Asian waters. Some intelligence analysts have warned that Indonesian and Filipino terrorist organisations have also realised the cash potential of piracy and are either directly implicated in pirate operations or collaborate with pirate gangs. The implications of terrorists acting as pirates go beyond the possibility for these groups to gain considerable revenue. Pirate attacks against vessels can also be used as a political tool to dissuade vessel passage through certain maritime bottlenecks. This is especially true in the case of the strategically important Malacca Straits where most Middle-East oil exports to Asia and most commerce between Asia and Europe pass. Major trade disruptions would result should the risk of piracy induce carriers to bypass this passage and prolong their trips around Indonesia.

Vulnerability of navigation: major world maritime routes, bottlenecks and areas of private activity



Risk factors: people

42. There are approximately 1 227 000 officers and ratings manning the merchant fleet[3]. Not all of these seafarers operate on internationally trading commercial vessels but a significant portion do. The terrorism-related risk involving this vast labour force is two-fold. As seen in the previous section, seafarers are often directly targeted (in many cases of piracy) and/or indirectly suffer from terror attacks targeting vessels (as in the case of the *Limberg*). The second risk factor is that some seafarers, or individuals posing as seafarers, may actually be accomplices to and/or members of terrorist groups. The latter is especially worrisome given that seafarers have traditionally been granted relatively liberal travel rights by governments through non-immigrant crew list visas, or simply upon presentation of their seafarer identity documents.

43. Data compiled on incidents of piracy reveals that a number of attacks were carried out with the help of an accomplice stowed away or serving among the ship's crew. A significant proportion of the world's commercial fleet is crewed through the assistance of professional crewing agencies that match candidates with ship owners/operators. While many of these agencies are reputable and ensure that the seafarers they represent fulfil international requirements and pass background checks, some do not. In the case of the latter agencies, it is feasible that seafarers with missing and/or falsified documents and with criminal backgrounds could be placed on ships[4]. Furthermore, several recent high-profile cases involving major registries and seafarer-supplying nations have shown the relative ease with which forged and/or falsified seafarer certificates and identity documents can be bought on the black market.

---

3 Total seafarers in 2000 according to the BIMCO/ISF Manpower Update Report.

4 As in the case of the MT Pulau Mas that was hijacked and subsequently used in 21 other pirate attacks as a "mother ship" communicating with a phoney crew member on board the target vessels (see http://www.cargolaw.com/presentations_pirates.html)

44. If unscrupulous persons are already aware of these subterfuges and are already operating in the world's fleet, it is not unreasonable to assume that terrorist groups are also aware of these possibilities and have, or are planning to, exploit them.

45. Ships operated or chartered by terrorists can also be used to deliver operatives into countries that otherwise would be difficult to enter. In many cases, intelligence agencies have been alarmed that commercial vessels have illegally discharged crew and/or passengers while at quay. While in many cases, these may simply be incidents of illegal immigration, some are genuinely worrisome.

Risk factors: financing/logistics support

46. That terrorist groups can operate single vessels or entire fleets in order to generate funds and support their logistics operations is no secret. In fact, one terrorist group's commercial maritime operations have been extensively documented.

47. Ever since the mid 1980's the Liberation Tigers of Tamil Eelam (LTTE), have developed and operated an extensive and profitable network of freight forwarders and ship operators. Current estimates of the LTTE's fleet size range from 10-12 reasonably well-maintained bulk freighters bearing Panamanian, Honduran or Liberian flags. The vessels are crewed by Tamils and owned by front companies in Asia. The majority of the cargo carried by the vessels is comprised of legitimate goods such as hardwood, tea, cement, fertilizer etc. and the vessels operate openly in the world shipping market. The funds generated through these activities are used to support the LTTE's ongoing war against the Sri Lankan government. However, approximately 5% of the cargo carried by these vessels is thought to be arms, ammunition and other war-related material necessary to carry out LTTE attacks in Sri Lanka. In some cases, the LTTE has also carried weapons and ammunition for other paying terrorist groups.

48. The LTTE's arms procurement network is highly sophisticated and depends on extensive knowledge of maritime trading practices and procedures. This knowledge has even been used to steal a major weapons shipment intended for the LTTE's adversary – Sri Lankan Defence Ministry – in a brazen case of documentary fraud (see Box).

Operational details on the use of maritime companies by the LTTE

On 23 May 1997, a Greek-registered freighter named Stillus Limassul left the Mozambican port of Beria for Sri Lanka carrying 32 400 81mm mortar bombs intended for that country's army. The USD 3 million arms deal had been arranged between officials of the Sri Lankan Defence Ministry and the government-owned, Chinese-built Zimbabwe Defence Industries (ZDI) and shipped by train to Beria. The Sri Lankan military never received the munitions…

Subsequent investigations revealed, however, that the Stillus Limassul was not included in Lloyds international shipping registry but was, in fact, owned by the LTTE itself. Further inquiries uncovered a paper trail that led to Ben Tsoi, an Israeli arms subcontractor who had arranged the mortar deal and apparently had been bribed by the Tigers to let one of their own freighters pick up the consignment. It is believed that Tsoi's company, L.B.J. Military Supplies, had persuaded ZDI to agree to the "sting" by providing false information to Colombo confirming that the shipment had been loaded, as scheduled, at the Mozambican port of Beira on 21 May 1997. Apparently, L.B.J Military Supplies then informed the Sri Lankan Government that the munitions were en route via Walvis Bay and Madagascar. By the time Colombo learned the full extent of what had happened, the mortars had been off-loaded and transshipped via smaller vessels to LTTE jungle bases off the Mullaitivu coast. A month later, the weapons were being used by the Tigers with devastating effect in the continuing battle for control of the A9 highway in northern Sri Lanka.

… Explosives have consistently been emphasized in [the LTTE's] global weapons procurement efforts. In the early days of the LTTE insurgency, these had been supplied directly to the LTTE. However, the curtailment of Indian support from 1987 onwards necessarily forced the group to seek new outlets further afield. Since the collapse of the Soviet Union in the early 1990s, the new favoured source has been Ukraine. One of the largest single consignments took place in August 1994 when an LTTE freighter, the MV Swene, left the Port of Nikoleyev laden with 60 tons of RDX and TNT explosive acquired from the Rubezone Chemicals plant. The transaction had been arranged through Carlton Trading, a LTTE front company located in Dhaka, which had produced a forged end-user certificate showing the Bangladeshi military as the approved recipient. The explosives were transported to the northeastern Sri Lankan coast and, protected by special Sea Tiger speed boats, off-loaded and transferred to several secret LTTE jungle bases. Some of these explosives (300-400 kg) were subsequently used in the massive January 1996 truck-bomb attack against the Central Bank building in Colombo – widely recognized as one of the most devastating terrorist assaults in history

Source: Chalk, Peter, Liberation Tigers of Tamil Eelam's (LTTE) International Organization and Operations – A Preliminary Analysis, Commentary No. 77, Canadian Security Intelligence Service, 17 March 2000.

49. The LTTE has been implicated in arms shipments to several international terrorist groups, including to the Harkat-ul-Mujahideen of Pakistan which is a member of the Al'Qaeda-linked International Islamic Front. It is not unreasonable to assume that Al'Qaeda and other terrorist groups have taken notice of the LTTE's use and manipulation of the maritime trading network for their purposes. As mentioned previously, it is believed that Al'Qaeda might already control a fleet of cargo vessels in order to generate revenue. Testimony emerging from the trial of the 1998 Embassy in Kenya has also revealed that Al'Qaeda operatives received bomb-making components via an Al'Qaeda controlled vessel. Tracking terrorist ownership and/or control of vessels, however, is a daunting task given the multiple possibilities for groups to obscure their true identities through weak vessel and/or corporate registration requirements.

Risk factors: trade disruption and security costs

50. Communiqués emerging from Al'Qaeda soon after the World Trade Center attacks revealed that one of the group's principal motivations was to inflict massive economic losses on the United States and its allies. Indeed, while the economic losses directly stemming from the attacks were extremely large, they were followed by medium- and long-term economic repercussions as costly security measures were quickly introduced (*e.g.* losses suffered by the airline industry following the 4-day closure of American airspace). Given that a) most of the world's trade travels by sea, b) most seaborne trade (by value) travels

in containers; and c) increased concentration in port activities means that most seaborne trade arrives in relatively few terminals, one can easily see the potential for major economic disruption following a terrorist attack on the maritime transport network.

51. As an illustration of the latter point, consider that the port of Long Beach/Los Angeles receives 42% of the total container imports (by value) to the United States or that 2 port areas (the Lower Mississippi Waterway and the Houston Ship Channel) receive 50% of the United States tanker imports, mostly of oil (both by value and weight). A co-ordinated attack on these ports/waterways could have tremendous short- and medium-term impacts on the United States economy. Likewise attacks on other major ports such as Hong Kong, Singapore, Rotterdam or Antwerp could have devastating impacts on both the regional and global economy.

3. COSTS OF A TERRORIST ATTACK ON MARITIME TRANSPORT

52. The potential direct cost of a terrorist attack on shipping or maritime infrastructure varies tremendously according to the scope of the attack, its target and its location. A single attack on a tanker, as in the case of the *Limberg*, could have relatively low direct costs (*e.g.* for repairs), whereas the detonation of an ammonia nitrate-carrying vessel in downtown New Orleans could result in tremendous loss of life and inflict massive property damage. The direct costs of such an attack, however, would likely be dwarfed by costs linked to reactions to the attack and disruptions engendered by emergency security measures.

53. As a case in point, we can turn to the costs stemming from the October 2002 *Limberg* attack. Immediately following the attack, underwriters tripled insurance premiums for vessels calling on Yemeni ports. These premiums, reaching as much as USD 300 000 per vessel (and USD 250 per TEU), led some lines to cut Yemen from their schedules and/or switch to ports in neighbouring countries despite attempts by the government to put in place a loss guarantee programme. Yemeni terminals saw throughput plummet (from 43 000 TEU in September 2002 to 3 000 TEU in November 2002) and have had to lay off workers. Local sources claim that as many as 3 000 people have lost their employment and government estimated losses stemming from attack are USD 15 million per month. Assuming that these losses are sustained over a 6-month period, they would account for nearly 1% Yemen's 2001 GDP.

54. Despite Al'Qaeda's claim of responsibility in the *Limberg* attack, the incident has generated relatively little disruption of global oil trade. This may be due to a perception that the risk to tankers is extremely localised and therefore easily mitigated (*e.g.* by bypassing Yemen and posting extra lookouts on deck). In the previous sections of this report, however, we have outlined scenarios of terrorist attacks – especially combining shipping containers and weapons of mass destruction – that pose global risks and are extremely difficult to mitigate. In order to get an idea of the magnitude of costs from such a major co-ordinated and sophisticated attack on ships and/or maritime infrastructure, we turn to two examples: the impacts from the October 2002 shut-down of United States west coast ports and the results of a recent strategic gaming exercise in the United States.

United States west coast port lock-out

55. In response to a dispute between labour and management, all American ports on the west coast of the United States Ports closed for 11 days in October of 2002. These ports handle approximately 42% of the United States maritime imports and exports by value and the losses from the lock-out were projected to reach in the billions of dollars. The port closure and the weeks of efforts necessary to clear the ensuing back-log imposed a high cost on American importers and exporters – how high exactly, however, has been subject to some debate.

56. Port management projected losses of approximately USD 19.4 billion for a ten-day lock-out with costs increasing exponentially as time went on. This estimate did not cover costs borne by non- American ports and manufacturers faced with container back-logs and increased warehousing costs. However, another study pointed out that the figure of USD 19.4 billion was more in line with the costs of *sinking* the

vessels heading for west coast ports rather than simply *delaying* them[5]. This report estimated potential losses borne by American workers, consumers and producers due to a 10-day lock-out to be approximately USD 466.9 million.

57. These figures are several orders of magnitude apart and do not accurately reflect the scope of costs likely to be imposed by a terrorist attack leading to a shut-down of these same ports. Not included in these figures are property damage costs (*e.g.* approximate construction costs for a modern 16 ha container terminal are USD 32 000 000 to which must be added land acquisition costs and container handling equipment including several cranes at USD 4.7 million apiece), costs related to port shut-downs in other countries, loss of life, insurance premia, etc.

58. As of yet there are no definitive *ex post* estimates of the total losses incurred due to the 11-day lockout but the current estimates of the port closure, as wide-ranging as they may be, should be seen as the absolute lower bound of potential costs stemming from a port-related terrorist attack.

59. What can be seen from these estimates, and from importers' actions before the lock-out, is that costs due to port closures are likely to rise exponentially with the duration of the closure up to a threshold at which radical changes in supply-chain strategies become cost-effective. Many American importers stated that a lock-out of several days and up to a duration of two weeks did not pose significant problems insofar as they had adjusted their inventory holdings beforehand. During that initial period importers with time-sensitive and perishable cargo faced the greatest losses. Beyond this window, however, many importers stated that they were willing to consider radical supply-chain changes in order to ensure their production/retail needs. These included paying for air transport and/or longer ocean transport through the Panama Canal and eastern coast of the United States, to changing their supplier base to non-Asian sources.

"Just-in-time" to "just-in-case"

60. Whereas importers were able to adjust their inventory holdings in the case of the west coast lockout because the disruption could be foreseen, they obviously could not do so in the event of an unpredictable terrorist attack. One response to this uncertainty has been for manufacturers to move slightly away from a reliance on "just-in-time" deliveries as they have increased their inventory holdings. David Closs of Michigan State University has estimated that in 2001 average large American companies held 1.36 months of inventory, down from 1.57 months in the early 1990's. He projects that this figure will rise to 1.43 months in 2002 as companies hold more "just-in-case" inventory in order to weather unpredictable trade flow disruptions. In effect, this means that, according to these estimates, the threat of terrorist attacks has wiped away approximately half of the logistics productivity gains realised in the United States over the past 10 years. Closs predicts that increased inventory holding could add USD 50 billion to USD 80 billion to business costs in the United States alone in 2002[6].

Conference board/Booz Allen Hamilton port security war game

61. In October of 2002 the American-based Conference Board and the consulting firm of Booz Allen Hamilton assembled 85 high-level government and industry representatives to test their responses to a major crisis involving the threat of terrorist attacks using containers shipped through North American

5 Anderson, Patrick, L. "Lost Earnings Due to the West Coast Port Shutdown--Preliminary Estimate", Working paper 2002-10, Anderson Economic Group LLC., October 2002.

6 See "The Friction Economy", *Fortune,* February 3, 2003 and Bowserbox, Donald and Closs, David. "Supply Chain Sustainability and Cost in the New War Economy." *Traffic World*, April 1, 2002.

ports. Government agencies represented included the Department of Transportation, American Customs, American Coast Guard, Department of Defence, Office of Homeland Security, intelligence agencies and port authorities. These policy-makers interacted with senior industry representatives from the transportation, distribution, logistics automobile, technology and food/beverage sectors. The war game scenario was based on a sophisticated and co-ordinated terrorist plot to smuggle in and detonate both radiological and conventional bombs (see war-game time-line below).

62. The principal motivation for undertaking the exercise was not to predict the exact impact from such an attack, but rather to identify barriers to better co-ordination among actors involved. For instance it became clear that emergency measures such as the immediate closure of all ports were easy to implement but could not be sustained very long. Authority for reversing the emergency measures, however, was relatively diffuse, and confusion over final authority in the matter lengthened the amount of time needed to get back to "normal" operations. Furthermore, even with 24-hour inspections assisted by the United States National Guard, only 20% of incoming containers could realistically be physically inspected. Measures that could have reduced the need for these inspections, such as measures that move inspections to origin ports and/or help to secure supply chains, could not be implemented in the time-frame of the war-game. The fact that many of the longer-term measures that could attenuate the impact of such a crisis are currently being implemented through multilateral (IMO, ILO) and bilateral initiatives would argue for the war game's estimate of a USD 58 billion impact should be treated as an upper bound. That estimate, in fact portrays the magnitude of potential costs likely to be faced in such a crisis *absent many of the security measures already being implemented and discussed further on*.

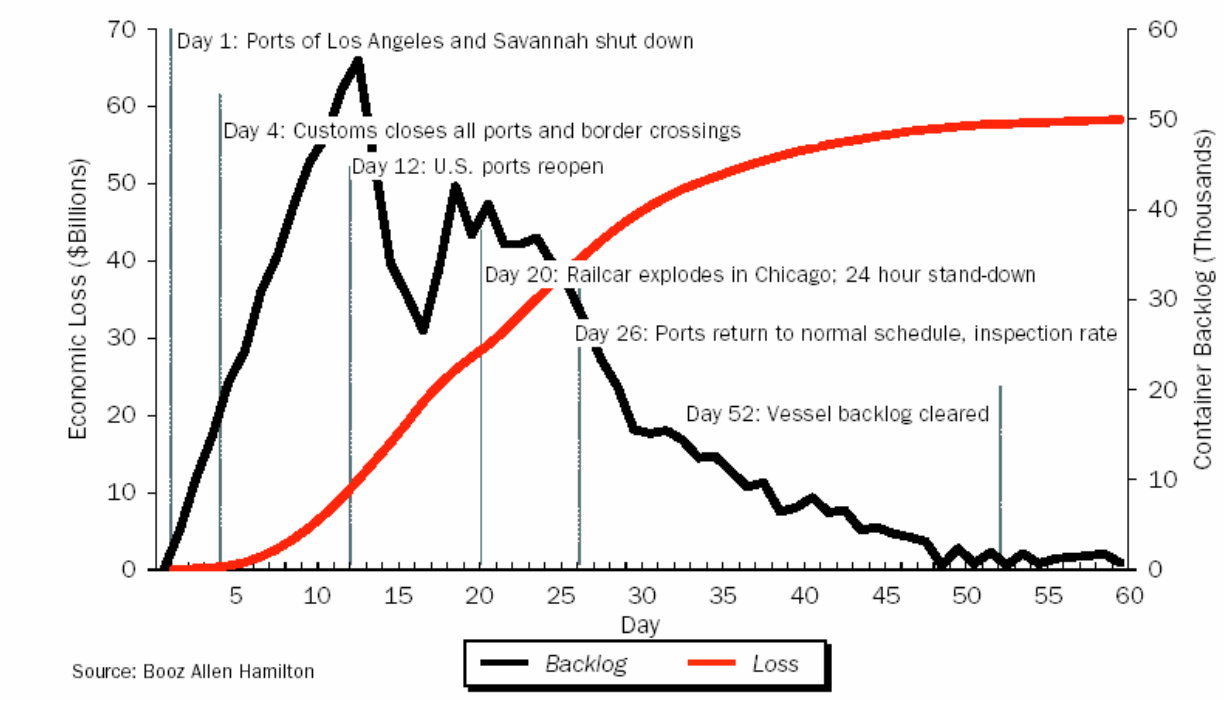
Conference board & Booz Allen Hamilton port security war game: timeline

Control actions		Participant decisions
Threat revealed of an unknown number of radiological bombs entering the United States via shipping containers. One such bomb discovered by accident at port of LA and 3 men on FBI Watch list arrested for suspicion of cargo theft at Port of Savannah	day 1	Ports of LA and Savannah shut down Carriers issue 24-hour stand-down, cargo is inspected and most carrier services are halted.
Public panic ensues in LA despite reassurances from the Port, mayor and Governor	day 2	
One of the suspects arrested in savannah is linked to Al'Qaeda; claims his mission was to pick up supplies in a container at the port and reveals that other teams may have similar missions at other American ports.	day 3	Carriers conduct voluntary self-inspection all trucks carrying containers in the United States.
Identical radiological bomb to the first one found while unpacking a container at a distribution centre near Minneapolis – container transported from Thailand to Port of Halifax and by truck to Minneapolis.	day 4	Customs closes all ports and border crossings indefinitely
DOW drops 500 points	day 5	California national Guard activated and set to be deployed
	days 6-7	
Gas prices skyrocket as port closures prevent ships from delivering fuel	day 8	Supply chains report inventory shortages and plant closures
	day 9	Port of LA requests that backlogged ships not targeted for inspection be sent to Canada and Mexico
Canada opens ports to ships unable to reach American ports	day 10	Industry-Government taskforce agree on container prioritisation protocols for container inspections
	day 11	
	day 12	All US ports open with 24 hr, 7-day operations Port of LA requests that ships return to its port
	days 12-17	
Radiation detected on two ships at Port of Savannah; USCG orders them back to sea for inspection	day 18	
	day 19	Ports return to normal operations (not 24hr/7 days)

Railcar carrying container of wine imported from France (entered US through port of NY/NJ) explodes in downtown Chicago Major indices plunge Wall Street trading halted and more than half of Fortune 500 firms issue earnings warnings	day 20	Carriers call for second 24-hour stand-down
	days 21-25	
	day 26	Port of LA returns to normal schedule and inspection rate
	day 27-51	
	day 52	All ports report vessel backlog cleared
	day 53-91	
	day 92	Container backlog stabilises Total losses as of day 92: USD 58 billion

PORT SECURITY WAR GAME—ECONOMIC IMPACT

Exhibit 4



Source: Booz Allen Hamilton

63. Terrorist attacks are by definition highly unpredictable. As such, attempts to quantify the economic impact of a theoretical attack are bound to be vague and deal *in orders of magnitude* rather than in precise sums. As such, little can be concluded as to the exact *quantitative* impact of a terrorist attack on, or using, the maritime transport network. Experience from Yemen, the American west coast port lockout and the recent Conference Board/Booz Allen Hamilton war gaming exercise do, however, point to the following conclusions as to the nature and magnitude of these costs:

- Potential direct costs of a terrorist attack are highly variable.
- Direct costs are likely to be dwarfed by indirect costs stemming from the attack and the reactions it provokes.
- Terrorist attacks targeting or using containers will likely have the largest secondary impacts,
- Costs linked to terror-related trade disruptions rise exponentially over time, up to a certain threshold where supply chains undergo radical changes.
- Total costs resulting from a sophisticated terrorist attack involving the maritime transport network and entailing major trade disruption will likely be measured in the billions, rather than in the millions, of dollars.
- Increased inventory costs resulting from uncertainty about trade flows are significant, possibly as high or higher than the total costs stemming from an attack.

64. Under normal circumstances, policy-makers facing a known risk should undertake a benefit-cost exercise to ensure that their responses to that risk do not impose greater costs than those imposed by the risk itself. The threat of terrorism, however, is difficult to label as "normal" circumstance and, as pointed out above, comprises so many unknown variables that traditional benefit-cost analysis is rendered nearly impossible. The conclusions outlined above cannot serve as a basis for comparison with the costs imposed by security measures except in their most rudimentary expression as indicative of the general scope and magnitude of potential costs likely to be incurred following a terrorist attack.

4. INTERNATIONAL CARGO: THREE CRITICAL FLOWS

65. Before examining the cost burden imposed by maritime transport security measures, it may be helpful to quickly describe the environment in which these measures will be implemented. This section examines the principal flows associated with the movement of maritime cargo in general – and of containerised cargo in particular.

66. Previous attempts to address maritime security in international fora have focused on the vessel itself and, at most, the immediate area surrounding the vessel in port. This focus was an outgrowth of the ship-focused mandate given to the International Maritime Organization – the UN body responsible for developing the common regulatory framework for international maritime transport. Inspired by similar approaches in the passenger aviation sector, this vessel- and passenger-centric approach has obvious limitations when dealing with the international movement of cargo by sea.

67. The reality today is that while most of the world's trade travels by sea, the ocean voyage is only one element in a complex chain. A typical door-to-door journey using a shipping container will involve the interaction of approximately 25 different actors, generate 30-40 documents, use 2-3 different modes and be handled at as many as 12-15 physical locations. The complex web of people, interactions, movements, and information associated with the international movement of goods can be broken down into three principal flows:

- Movement of goods from place to place.
- Movement of custody from person to person.
- Movement of information regarding the cargo.

Places and modes

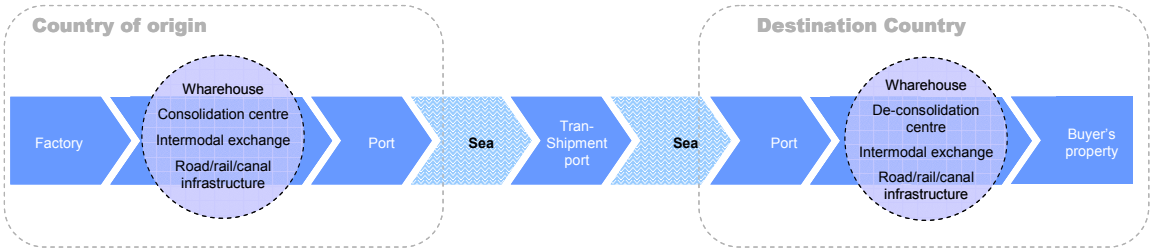
68. The first chain involves the physical movement of cargo from place to place and from mode to mode. This is the most tangible chain from a security perspective. Once suspected and/or confirmed, threats can be localised along this chain and actions can be taken to physically neutralise the threat. Knowing where a shipment originated, how it has travelled, where it can be localised and whether its integrity has been compromised are key questions for security agencies intent on intercepting threatening cargo. As such, it is important for policy-makers to also be aware of the physical reality of the cargo logistics chain.

69. Cargo originates from the manufacturer's premises. Here it is palletised and/or packed into a container and transported by road/rail either directly to a port, or to an intermediary's premises. In the latter case, the shipment will be consolidated with others and transported to a multi-modal staging area or to a port. While in transit, the container may be stationary for various periods of time as trucks are stopped on the roadside and/or container-carrying trains are being assembled in freight yards. Once in port, the container is sent to a staging area before it is placed immediately next to the vessel at quay. Even within the port area, a container may be moved several times as required by the port operator and/or customs. After being placed on board a ship, the container can be removed and trans-shipped in another port onto another vessel before arriving at its destination port. Here again, the container may be moved several times

for customs clearance and into temporary storage areas while waiting to be picked up. Carried by road, rail or inland waterway to its final destination, the shipment may again transit through several intermediaries' facilities where the container is unpacked and the palletised shipments it contains are distributed.

70. The logistics chain described above is not uniformly secure and the level of protection offered containers and their contents can vary tremendously from node to node and among modes. The risk of security breaches at any one of its links compromises the security of the whole chain and imposes additional costs as additional security checks must be put in place to compensate. Also, the level of protection present at different nodes and in transit is often directly related to the value of the goods being shipped. A major electronics manufacturer will invest much more in securing his/her supply chain than will a small low-volume exporter of inexpensive porcelain objects. And even in cases where relatively high levels of protection are put in place, cargo theft remains a problem. There are literally tens of thousands "entry points" along modern logistics chains that could be exploited by terrorist groups.

International Container Logistics Chain Vulnerability Assessment:
Places in the logistics chain



Actors in the logistics chain

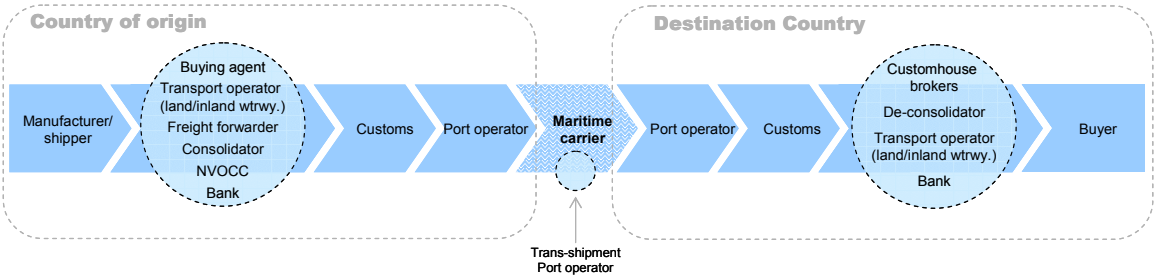
71. Every trade transaction involves dozens of primary agents. In addition, hundreds of people can potentially come into contact with containers and their contents along the logistics chain described above. Understanding the flow of custody for the contents of a container and identifying and ensuring the security clearance of people who come into contact with containers are key challenges facing governments world-wide.

72. At the beginning of every container journey is a buyer and an an originating shipper – most often a manufacturer. There are hundreds of thousands of manufacturers around the world and many of them are active in international trade. These manufacturers may produce high enough volumes or be located near enough to a port that they can ship full container loads directly. Most however, produce less than container load (LCL) shipments that must be consolidated before being shipped by sea.

73. Buying agents and/or freight forwarders serve as the most common intermediaries between originating shippers and ocean carriers. There are approximately 40 000 freight forwarders world-wide in an industry employing 8 to 10 million people. While many freight forwarders handle full container load shipments for their clients, their principal task revolves around the assembly and consolidation of LCL shipments into full containers. They also facilitate the entire international trade transaction by serving as agents for the cargo with other transport intermediaries, customs and other government agencies, banks and receiving parties. In some cases, the forwarder will negotiate each transaction on behalf of the shipper while in other cases, the forwarder will be the principal agent contracting with the shipper.

74. While forwarders offer multiple services in the logistics chain, other parties also offer these individually as well – *e.g.* customs brokers, truckers/rail carriers, warehouse agents, etc. Furthermore, when in transit or in port areas, hundreds of warehouse/staging yard/port workers may have physical access to shipping containers. Each service offered along the logistics chain implies the involvement of a company comprised of several, to several hundred, people – any one of whom may potentially have nefarious intentions.

International Container Logistics Chain Vulnerability Assessment:
People/Actors involved



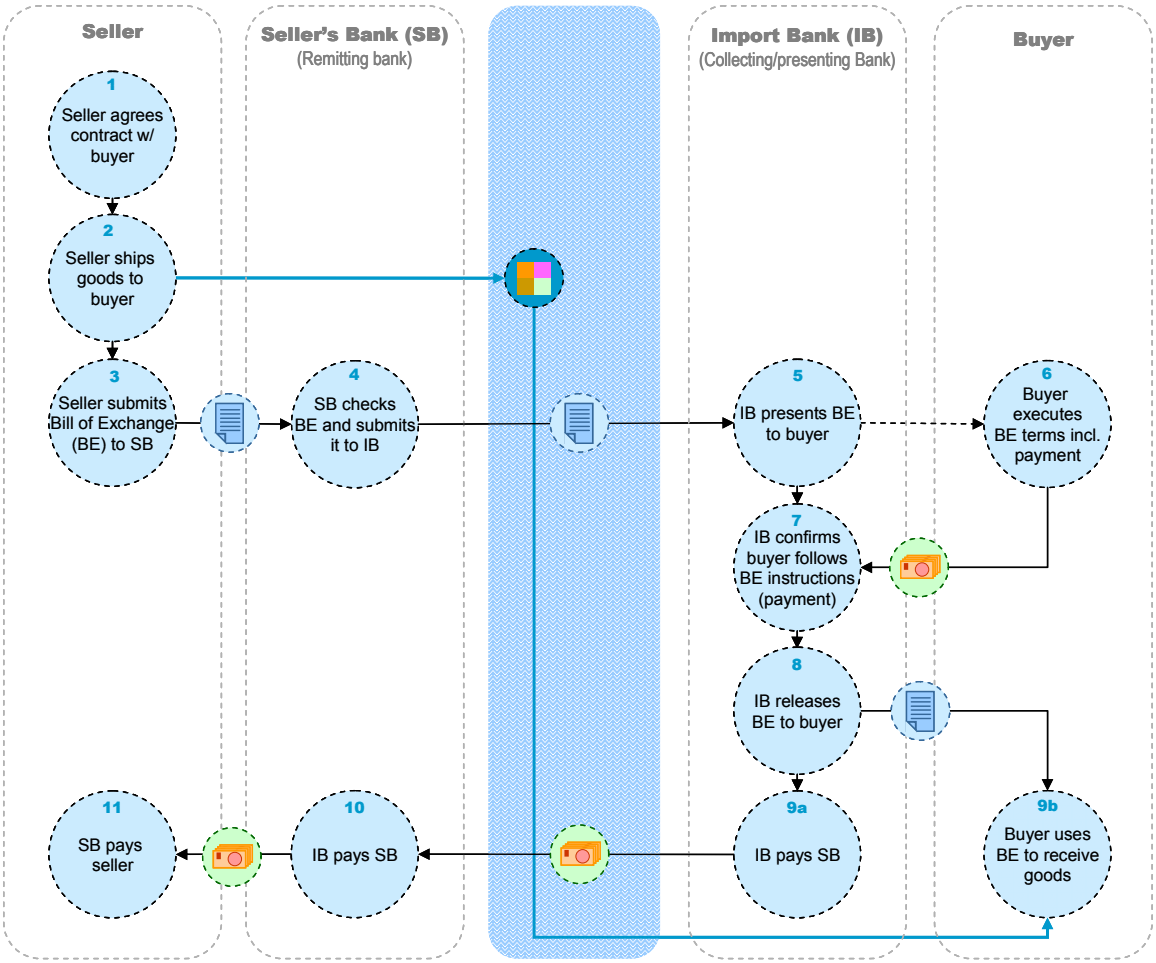
75. As with the security of nodes in the logistics chain, the level of scrutiny given every worker potentially coming into contact with containers and their contents varies considerably among companies and countries. While some companies may require extensive background checks for their workers, many do not. But even background checks do not represent a panacea as an entire company can be owned or operated by a terrorist group as has been seen in the past with the LTTE (see box on page 14). The principal foil in such a case – where a terrorist group runs a "legitimate" operation for several years to build a reputation of trust – is better intelligence and transparency in company ownership disclosure requirements.

Cargo information flow

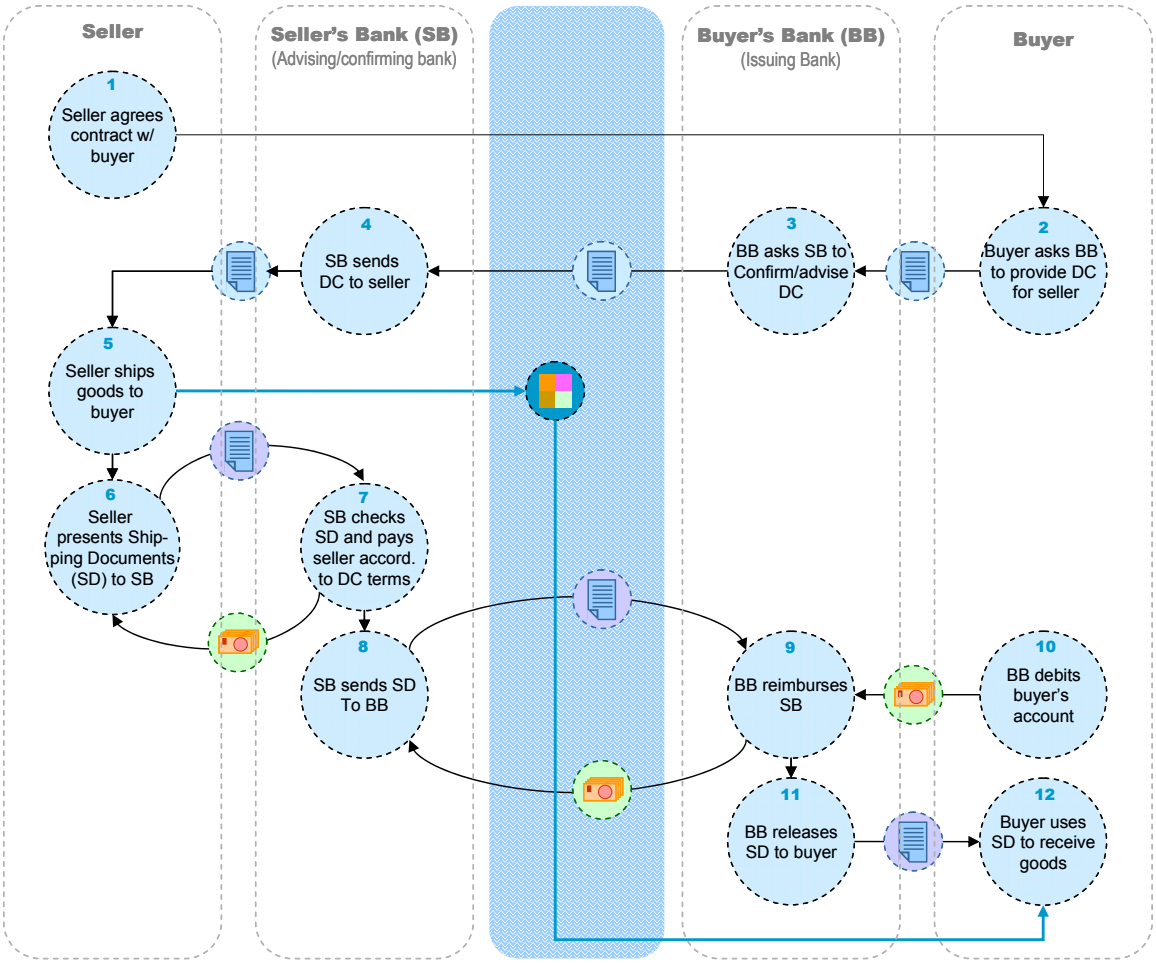
76. International trade is impossible without the secure transmission of key pieces of information among dozens of actors who may have never met. These information requirements include the specification of the good to be shipped, the quantity, the number packed onto each pallet and into each container, details about custody/liability, information regarding the timing and responsibility for payment, information regarding who is authorised to act on behalf of the shipper and/or receiver, etc. As noted above each transaction can involve up to 40 separate documents – some of them duplicative of others (e.g. in the case of a forwarder issuing a bill of lading that is duplicated by the ocean carrier's bill of lading). Because customs and security agencies rely on this information in order to make informed judgements on which containers to inspect, small manipulations along this chain can have potentially serious consequences. The risk is real as attests to the incidence of documentary fraud used for cargo theft. Furthermore this risk is compounded because most of the information flow in international trade is still paper-based, costly and inefficient.

77. There are many scenarios for import-export transactions but we will illustrate two of the most common to give an idea of typical paper-based information flows. The first entails a buyer and seller transacting through their respective banks using a negotiable bill of exchange and the second represents the two operating the same transaction using a documentary credit.

Flow of information/money: bill of exchange (BE)



Flow of information/money: documentary credit (DC)



78. These represent the purely commercial transactions involved in the two instances. In addition to these are the security-related information flows that operate between shippers, freight forwarders, carriers and customs/security authorities. The level of automation for the latter vary widely throughout the world with some countries boasting high rates of electronic data transmittal (*e.g.* the American Customs claims that 90% of import documents are filed electronically through their Automated Manifest System). However, in many cases what is being transmitted electronically is simply an image of a paper document with little real digital value. In other cases, data on shipments is being re-copied by carriers and some forwarders before being sent on to customs authorities (until very recently, only carriers could submit documents electronically to American Customs). While many in the industry claim that transforming the paper-based chain to an electronic one would be prohibitively expensive, continued decreases in the cost of computing equipment and increasing computer literacy world-wide might make such a change feasible sooner than later. A switch to an electronic-based information system underpinning world trade would likely be accompanied by a number of new security loopholes but, at least from the perspective of integrating information on shipments, shippers and intermediaries with security-related databases, the switch could potentially reduce the vulnerability of the system to be misused by terrorists.

5. MARITIME SECURITY: COST CONSIDERATIONS FOR ENACTED AND PROPOSED SECURITY MEASURES

79. Very quickly after the World Trade Center attacks, attention shifted from aviation to maritime security as it became evident that the vulnerabilities detailed earlier in this report could potentially be targeted by organised terrorist groups such as Al'Qaeda. Following the unprecedented security measures taken by the United States *(e.g.* the closing of its national airspace for 4 days), a concerted international effort was undertaken to rapidly develop a strategy to reduce the danger from terrorist acts on the maritime transport system. Four principal elements emerged as part of that strategy; the need to track vessels, the need to address the security of vessels and ports, the need to verify and authenticate the identity of seafarers and the need to ensure the integrity of containerised cargo. These four elements formed the basis of a draft proposal to the IMO that was reviewed at a special meeting Maritime Safety working group in February 2002. After some changes – notably the removal of IMO action on seafarer identity documents (transferred to the International Labour Organization) – the strategy was accepted at the September meeting of the working group and adopted at the IMO Maritime Safety Committee (MSC 76) meeting in December 2002.

80. The IMO package of security measures included changes to the Safety of Life at Sea (SOLAS) Convention – including a new Chapter X1-2 that solely addresses ship security – and a new, 2-part, International Ship and Port Facility Security Code (ISPS) Code. Part "A" of this code details mandatory measures to be taken by contracting governments, shipowners, and ports and part "B" lists voluntary measures to enhance maritime security. The changes and additions adopted at MSC 76 in December 2002 will come into force on July 1st, 2004.

81. Beyond the compulsory elements of the IMO package are a number of mandatory national initiatives, for the most part taken by the United States. These are binding for vessels and cargoes leaving, arriving and passing through the United States. Most of these measures are supplemental to the IMO package with the notable exception being that the United States currently (March 2003) interprets the "voluntary" recommended guidance comprised in part "B" of the ISPS code as being mandatory for American -bound vessels insofar as these vessels must fully account for the guidance provided..

82. Finally, the United States has proposed a series of voluntary programmes aimed at improving ship and port security. While not binding, these measures have been put into place in order to facilitate the movement of cargo by participating ports, carriers and companies, and, as such, can potentially have a determinant competitive impact. Because of this, the cost considerations of the two principal American voluntary programmes – the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT) – will be examined.

Mandatory measures: SOLAS chapter X1-2 and the international ship and port facility security code

Scope

83. The compulsory security measures adopted at MSC 76 are applicable to the internationally trading fleet of vessels over 500 gross tonnes – for the purposes of this report, we will assume this population to be 43 291 vessels which corresponds to Lloyd's Register estimation of the size of the world's

cargo-carrying fleet (of over 1000 gt) in 2001. The security measures adopted at the IMO are also applicable to passenger ships, mobile offshore craft and other merchant vessels of between 500 and 1000 gross tonnes. While security costs associated with these vessels are important, especially for passenger vessels, they fall beyond the scope of this report and will not be included in the analysis.

Measures

84. The measures prescribed in SOLAS XI and the ISPS Code can be broadly broken down into five major categories according to their focus. These are:

- Measures targeting contracting governments.
- Measures targeting ships.
- Measures targeting maritime carrier companies.
- Measures targeting ports.
- Certification/documentary requirements.

Measures targeting contracting governments

85. The principal responsibilities of contracting governments under the new IMO security regulations are to determine and set security levels (*e.g.* 1=low, 2=medium and 3=high) and communicate information regarding security levels to ships flying their flag, to port facilities within their territory and to foreign flag vessels in, or about to enter ports within their territory. These alert levels are associated with a number of security procedures that are to be implemented by ships crews and port operators in order to ensure that security measures are commensurate with the level of risk implied by the alert.

86. While some expense is associated with the development of these security levels, it is likely that this cost is small and would be paid for by the government agency responsible for defence or maritime security. The greater cost would likely stem from the application of the security levels – especially from the declaration of a level 2 or level 3 alert. Part B of the ISPS Code outlines suggested measures to be taken by vessels, crews and ports when operating under levels 2 and 3 (see Annex I) and gives some idea of the scope of costs/disruptions that would be attributable to these alerts. While the majority of the actions outlined under security level 2 imply labour, manning and time costs (e.g. when screening cargo), those detailed in section 3 could have major disruptive effects (*e.g.* evacuating the ship, stopping all cargo loading operations in port, etc). Extended operations under level 2 alerts punctuated by some level 3 alerts, therefore, would generate relatively elevated indirect costs – with the exact level of these contingents on the duration of the security alerts and the number of ports declaring them.

87. Contracting governments also have other responsibilities under SOLAS XI-2 that could entail material expenses. These include:

- Determining which port facilities are required to designate a Port Facility Security Officer.
- Ensuring completion and approval of a Port Facility Security Assessment and the Port Facility Security Plan for each port facility that serves ships engaged on international voyages.
- Approving the Ship Security Plans and amendments to previously approved plans.

- Verifying the compliance of ships and issuing the International Ship Security Certificate, and any subsequent amendments; and exercising control and compliance measures.
- Communicating information to the International Maritime Organization and to the shipping and port industries.

➢ Direct costs: low Indirect costs: potentially very large

Measures targeting ships

88. The modifications to SOLAS undertaken at MSC 76 included three ship-related provisions. These were the advancement of the date at which all ships were to be equipped with Automatic Identification Systems (AIS), the permanent marking and display of the ship's unique identification number and the installation of a ship security alert system.

Automatic identification systems (AIS)

89. Automatic Identification Systems are ship-borne communication devices that communicate to other AIS transponders and shore-based facilities basic information regarding the ship's identity, position, heading and speed. Primarily designed to enhance the safety of navigation in crowded areas, AIS systems can also be used by states to monitor the movements of ships that are suspected to present a security risk. Because of this, MSC 76 agreed on moving forward the agreed calendar for vessels to be equipped with AIS to December 2004 at the latest. Passenger vessels and large tankers (over 50 000gt) were already required to have AIS as soon as July 2003 and other vessels trading internationally were scheduled to equip themselves with AIS from July 2003 to July 2007, depending on their size. The basic price for an AIS transponder ranges from USD 10 000 to USD 20 000 and so the cost to equip the entire international commercial fleet is approximately USD 649.3 million (at USD 15 000 per transponder). This amount, however, should not be seen as a security cost *per se* given that AIS requirements were already in place before MSC 76. If there is a security-related component to the costs of AIS, it covers the opportunity costs for money spent on AIS now, as opposed to according to the original AIS implementation schedule. Also, another ISPS-related cost might be that shipowners will equip their vessels with simple AIS systems in line with the ISPS requirements/deadline, only to have to upgrade these for more sophisticated systems that comply to the original AIS specification as these come on line at a later date.

90. The other cost associated with AIS is the development of shore-based reception facilities. These will generally be built and operated by governments as an extension of their traditional safety of navigation roles. It is premature at this time to make an estimation of these costs since shore-based reception facilities are not required under SOLAS. It is equally unclear if and how governments may seek to recoup these costs from users.

➢ Direct costs: ~USD 649.3 million Indirect costs (shore stations): undetermined

Ship identification number

91. SOLAS Chapter X 1 also requires vessels to prominently and permanently display their unique identification number. This number must be displayed no later than following the ship's first dry-docking after July 1, 2004 and must be embossed, punched and/or cut into the ship. Industry sources estimate this cost to be in the order of USD 5 000 although this expense might be folded into scheduled re-painting operations during the vessels' scheduled dry-docking.

- Direct Costs: USD 21.6 million Indirect costs: nil

Ship security alert system

92. Finally, SOLAS Chapter X1 also specified that all passenger ships, high-speed cargo vessels, chemical tankers, oil tankers and gas carriers of more than 500 gt must be fitted with a Ship Security Alert System no later than the first radio equipment survey after July 1, 2004. Other cargo vessels of more than 500 gt will have to do the same no later than the first radio equipment survey after July 1, 2006. According to the new rule, the security alert system will:

- Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Flag administration**,** which in these circumstances may include the company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised.
- Not send the ship security alert to any other ships.
- Not raise any alarm on-board the ship.
- Continue the ship security alert until deactivated and/or reset.
- Be capable of being activated from the navigation bridge and in at least one other location.
- Conform to performance standards not inferior to those adopted by the IMO.

93. The USCG estimates that such a system will cost approximately USD 2 000 apiece and will require approximately USD 100 in maintenance per year. This puts the estimated cost of ship alert system acquisition at approximately USD 86.5 million (~USD 40.1 million for the 2004 deadline and ~USD 46.4 million for the 2006 deadline). Yearly fleet-wide maintenance costs are approximately USD 4.3 million.

- Direct costs: ~USD 86.5 million Yearly maintenance costs: ~USD 4.3

Measures targeting companies

94. SOLAS Chapter X1-2 and the ISPS Code set out a number of security responsibilities incumbent to vessel-owning and/or operating companies. The principal responsibility for these companies is to ensure that each vessel it operates obtains an International Ship Security Certificate (ISSC). This certificate is to be issued by the Flag Administration or by a Recognised Security Organisation (RSO), such as a classification society, on the Flag State's behalf. The IMO rules outline six steps required for the issuance of a Ship Security Certificate. These are:

- Designating a Company Security Officer (CSO).
- Undertaking a Ship Security Assessment (SSA), including an on-site visit, for every vessel to be issued a SSC.
- Developing a Flag-State-approved Ship Security Plan (SSP) that references the individual ship's SSA and incorporates all of the elements included in part "A" of the ISPS Code.
- Designating a Ship Security Officer (SSO).

- Providing adequate training for the CSO, SSO and crew and ensuring that adequate drills and exercises are carried out.

- Ensuring that vessels are equipped to carry out the security procedures outlined in their SSP's.

- Ensuring adequate security-related record-keeping as outlined in part "A" of the ISPS Code.

Company security officer

95. While a company may designate several company security officers, every company operating vessels must have at least one CSO who is ultimately responsible for company and ship compliance with the new IMO security rules. These rules identify 13 specific responsibilities incumbent upon the CSO ranging from carrying out/organising CSA's for all vessels to ensuring training for SSO's, and crews (see Appendix 2 for details). The IMO rules do not specify whether a CSO must be a dedicated position within the company or whether the responsibilities of the CSO can be assigned to an existing position within the company. Initial feedback from industry is mixed – larger ship operators will likely (if they have not already done so) create a new CSO post while smaller operators might seek to assign those duties to an existing post.

96. The United States Coast Guard assesses the cost of a CSO for a large American-based company to be USD 150 000 per year and USD 37 500 per year for a small American-based company. For the purposes of this paper, we will consider that large firms in the international shipping sector are generally competing against each other in the international job market and face similar labour costs for upper management. Therefore we will assume that a. large international shipping companies will a) create a dedicated CSO post and that b) the annual cost of a CSO for a large internationally trading operator is USD 150 000 per year. Furthermore, based on USCG figures, we will assume the following costs for large ship operators: CSO training (USD 3 500/yr) and training of other key crew (USD 5 000/year).

97. Another complicating factor is determining the size cut-off between large and small companies. For the purposes of this study, we will assume a "large" company operates more than 10 vessels and a "small" company less than ten. Fairplay/Lloyd's List counts 12 987 ship operators throughout the world in their online world shipping directory. Many of these, however, are solely domestic operators. We will assume that 50% (6 494) are active in international trades. Precise estimates on the number of companies controlling ten or more vessels are difficult to make given that, for liability purposes, many vessels are owned by "one ship" companies. Many of these companies, however, are effectively controlled by the same entity. Past work on ISM Code compliance indicates that as many as 50% of these companies (3 247) may indeed control 10 or more vessels. Thus the cost related to the hiring of a CSO and training appropriate staff for "large" companies is approximately USD 514.6 million per year.

98. The cost of a CSO for a smaller company is more problematic because these companies tend to operate in local labour markets for which data is relatively scarce in the shipping sector. Furthermore, it is unclear to what extent CSO duties will be assigned to existing posts within smaller companies. Industry sources estimate these costs to be in the order of USD 100 to USD 200 million per year. For the purposes of this report, we will assume these costs to be approximately USD 150 million per year.

- Direct costs (large companies): ~USD 514.6 million/yr

- Direct costs (small companies): ~USD 150 million/yr

Ship security assessment

- Part "A" of the ISPS Code sets out the requirements of the mandatory Ship Security Assessment. The SSA must include an on-site visit for each vessel and accomplish the following, at a minimum:
- Identification of existing security measures, procedures and operations.
- Identification of and evaluation of key ship-board operations that are important to protect.
- Identification of possible threats to key ship-board operations and the likelihood of their occurrence, in order to establish and prioritize security measures.
- Identify weaknesses, including those related to crew/personnel ("human factors"), in the infrastructure, policies and procedures for ship-board security.

99. The SSA is a fairly comprehensive review of the ship's particularities, trading patterns and vulnerabilities and should outline preventative counter-measures to address the latter. The SSA should address the physical security of the vessel (including access points), the structural integrity of the vessel (including high-risk areas to be designated as restricted access), crew protection systems, security procedures, radio, computer and other communication systems and ship stores/cargo areas. The USCG estimates that completing a SSA requires 16 hours (2 8-hour days) at an hourly rate of USD 100. Industry sources believe this to be a low estimate and consider that a SSA would require 3 to 4 days. We will assume that such an audit requires 3 8-hour days at an hourly rate of USD 100. We will further assume this cost to be representative of international costs as charged by classification societies and/or other security assessment services who will most likely be undertaking a majority of SSA's. Thus, the total international fleet costs for developing SSA's can be estimated to be approximately USD 103.9 million.

- Direct costs: ~USD 103.9 million

Ship security plan

100. The ISPS code requires each ship to carry on board a Ship Security Plan that has been derived from the SSA. This plan must be approved by the Flag Administration and or an approved RSO. Furthermore, this plan cannot be approved by the same RSO that has elaborated its content. The SSP must make provisions to address security procedures and policies for each of the three alert levels determined by Contracting Governments. The SSP is a "living" document that can and should be re-assessed as conditions warrant. At a minimum, the plan should address the following 13 elements:

- Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship.
- Identification of the restricted areas and measures for the prevention of unauthorized access to them.
- Measures for the prevention of unauthorized access to the ship.
- Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface.
- Procedures for responding to any security instructions Contracting Governments may give at security level 3.
- Procedures for evacuation in case of security threats or breaches of security.

- Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects.
- Procedures for auditing the security activities.
- Procedures for training, drills and exercises associated with the plan.
- Procedures for interfacing with port facility security activities.
- Procedures for the periodic review of the plan and for updating.
- Procedures for reporting security incidents.
- Identification of the ship security officer.
- Identification of the company security officer including with 24-hour contact details.
- Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board, if any.
- Frequency for testing or calibration any security equipment provided on board,
- Identification of the locations where the ship security alert system activation points are provided.
- Procedures, instructions and guidance on the use of the ship security alert system including the testing, activation, deactivation and resetting and to limit false alerts.

101. Feedback from industry indicates that SSP will likely be elaborated along a set template or series of templates that are modified according to each vessel under review. As such, elaborating a SSP will take less time and resources than carry out a SSA. These SSP's will in many cases be carried out and/or audited by classification societies. The USCG estimates 4 hours per SSP at a rate of USD 100/hr. Industry sources dispute this figure and believe an SSP will take at least 20 hrs. For the purposes of this report, we will assume that an SSP will require 12 hours at USD 100/hr. Thus the total cost of elaborating SSP's for the internationally trading cargo fleet is approximately USD 51.9 million.

- Direct costs: ~USD 51.9 million

Ship security officer

102. Beyond the other company-targeted provisions of the ISPS Code, companies are also required to designate and train a Ship Security Officer for every vessel the company operates. This officer will be responsible for all security-related aspects of the vessel's operation, including the implementation of the SSP for each security alert level. At a minimum, the SSO will be responsible for the following 10 duties:

- Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained.
- Maintaining and supervising the implementation of the ship security plan, including any amendments to the plan.
- Coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers.
- Proposing modifications to the ship security plan.

- Reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions.
- Enhancing security awareness and vigilance on board.
- Ensuring that adequate training has been provided to shipboard personnel, as appropriate.
- Reporting all security incidents.

103. At the time of this report's writing, only 3 months after MSC 76, it had already become apparent that the vast majority of ship operators will fold the responsibilities of the SSO into an existing post onboard – most likely that of the Master. For the purposes of this analysis we assume that security duties occupy the Master 5 days per year (principally for security inspections). Using the International Transport Workers' Federation's Grade B benchmark wage rate of USD 4 080/month, we estimate SSO costs for the internationally-trading commercial fleet to be approximately USD 29 million per year.

- Direct costs: ~USD 29 million/year

Ship security training and drills

104. The ISPS code requires companies to ensure that CSO's, other appropriate, shore-based personnel, SSO's and crewmembers with security duties receive training such that they may carry out their security related duties. The costs of this training were outlined on page 32 (discussion of Company Security Officers). The ISPS code also requires periodic training drills to ensure that crew know and understand how to respond to security incidents and alerts. Part "B" of the ISPS Code suggests that these drills occur at least once every three months and should involve the entire crew. For the purpose of this exercise, we will assume an average crew size of 15 plus one Master and a security drill duration of 1 hour, 4 times per year. To determine crew labour costs, we will use the International Transport Workers' Federation's Grade B benchmark monthly wage rate of USD 4 082 for Masters and USD 1 300 for other crew. Thus, the estimated cost of security drills on the world's internationally trading commercial fleet is approximately USD 16.8 million.

- Direct costs: ~USD 16.8 million/year

Vessel security equipment

105. Part "A" of the ISPS Code does not list specific equipment that must be carried on board in order to ensure the vessel's security at each of the different security alert levels. In reading the detailed suggestions in part "B" of the ISPS Code (which, again, is not compulsory with the exception of vessels in the American trades), however, one can get an idea of the general equipment needs that the IMO rules imply. The United States Coast Guard has detailed the equipment requirements that it feels would enable vessels to comply with the guidance given in part "B" of the ISPS Code. These are differentiated by vessel type between tankers and other freight vessels and by investment and maintenance costs as outlined in the table below.

Item	Initial investment			Annual maintenance	
	Number	Cost/item (USD)	Total cost (USD)	Cost/item (USD)	Total cost USD)
Tanker					
Hand-held metal detector	1	200	200	10	10
Hand-held Radio	5	200	1 000	10	50
Lock	10	300	3 000	15	150
Light	5	400	2 000	20	100
Auto-intrusion alarm	5	500	2 500	25	125
Freight Ship					
Hand-held metal detector	2	200	400	10	20
Hand-held Radio	5	200	1 000	10	50
Lock	10	300	3 000	15	150
Light	5	400	2 000	20	100
Auto-intrusion alarm	5	500	2 500	25	125
Portable vapour detector (for explosives)	1	8 000	8 000	400	400

106. It is unlikely that security equipment expenditures for the worldwide fleet of commercial vessels will conform to the costs outlined above, principally because these costs assume all of the guidance in part "B" of the ISPS code to be mandatory. For the purposes of this exercise, we will assume that commercial vessels visiting the United States will conform to the above expenditure schedule as will container vessels trading internationally (because of the heightened risk their cargos pose).

107. The United States Department of Transport keeps statistics on vessels of over 10 000 dwt visiting the United States[7] (as opposed to Lloyd's which compiles data on the merchant fleet of over 1 000 gt). In 2000, 6 353 vessels of over 10 000 dwt visited American ports, of which 1 577 were oil, gas or chemical tankers and 907 were container vessels. This represents 48%, 44% and 44% respectively of the world commercial fleet of over 10 000 dwt (13 235 vessels in 2000). This also represents 14%, 13% and 35%, respectively of the world commercial fleet of over 1 000 gt. Since data is lacking on the number of smaller vessels visiting the United States (1 000 gt to 10 000 dwt), we will take the latter figures as a conservative estimate of the number of vessels visiting American ports and will assign the costs outlined in the above schedule only to these. We will further assume that the fleet distribution in 2000 (for which we have American data) is similar to the fleet distribution for 2001 (the latest reporting year for Lloyd's). For other vessels, we will assume that the following equipment needs will be sufficient to comply with the vessels' SSP: 0 hand-held metal detectors, 3 hand-held radios, 5 locks, 5 lights, 2 auto-intrusion alarms and 0 portable vapour detectors. Thus we estimate the total initial investment in equipment necessary to comply with the ISPS code (and the American's interpretation of the Code's part "B") to be approximately USD 304.4 million. We also estimate the yearly maintenance costs of ISPS-related equipment to be approximately USD 15.2 million.

[7] "Vessel Calls at US Ports 2000", MARAD Office of Statistical and Economic Analysis, January 2002

	Initial Investment per Vessel (USD)	Annual Maintenance per Vessel (USD)	Number of vessels (2001)	Total Initial Investment (USD)	Total annual maintenance (USD)
American Trading Tankers	8 700	435	1 587	13 805 852	690 293
American Trading Freight vessels (non-container)	16 900	845	3 852	65 098 757	3 254 938
World Container Fleet	16 900	845	2 756	46 576 400	2 328 820
Non- American Trading Tankers	5 100	255	9 496	48 430 214	2 421 511
Non- American Trading Freight Vessels (non Container)	5 100	255	25 600	130 560 013	6 528 001
Total			43 291	304 471 236	15 223 562

- Direct costs: ~USD 304.4 million Yearly maintenance costs: ~USD 15.2 million

Record-keeping

108. Finally, the ISPS Code requires ships to keep on board records of the following activities for a period set by the Flag Administration:

- Training, drills and exercises.
- Security threats and security incidents.
- Breaches of security.
- Changes in security level.
- Communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been.
- Internal audits and reviews of security activities.
- Periodic review of the ship security assessment.
- Periodic review of the ship security plan.
- Implementation of any amendments to the plan.
- Maintenance, calibration and testing of any security security equipment provided on board, including testing of the ship security alert system.

109. At the time of this report's writing, there is no experience with security-related record keeping on-board vessels. However, we will assume for the purpose of this analysis that the amount of time spent keeping and updating security records will be negligible and assign no cost to this element of the ISPS Code.

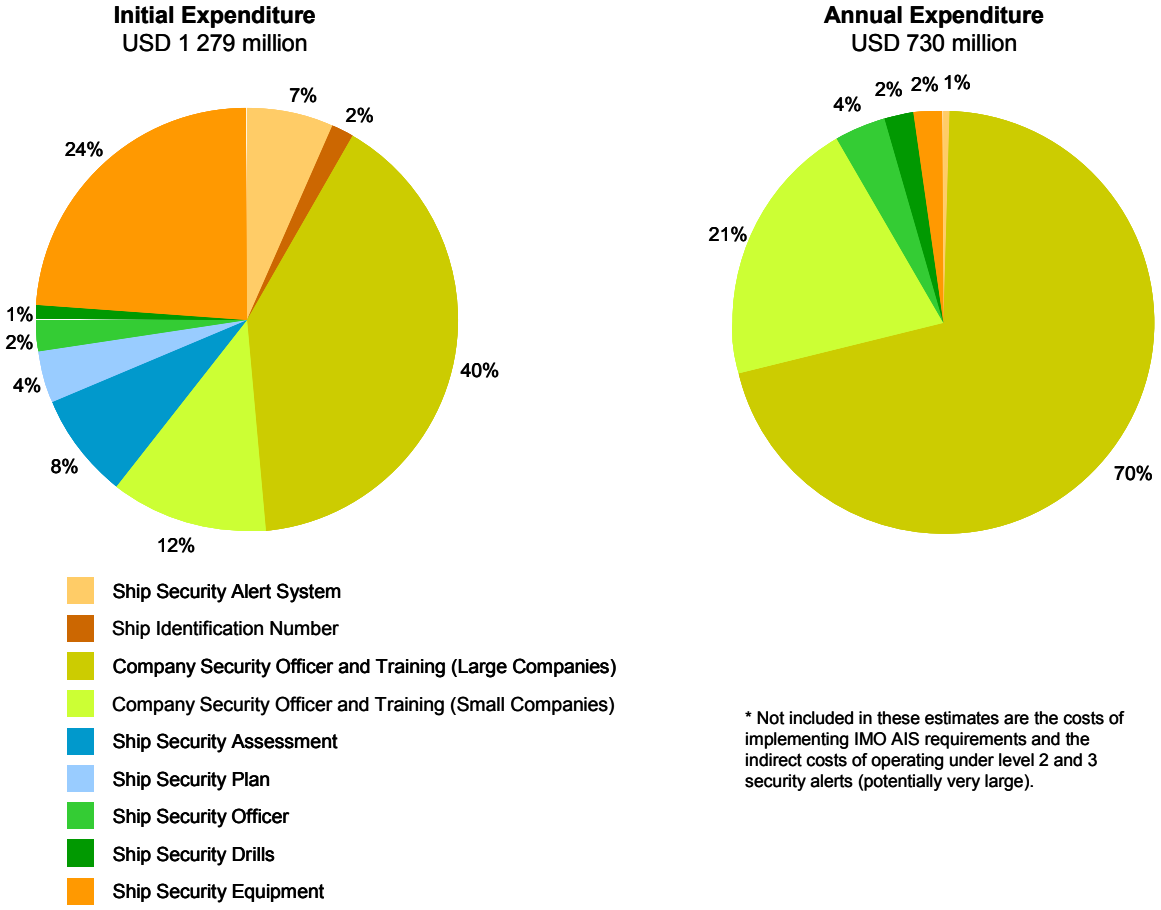
- Direct costs: low

Conclusion: SOLAS/ISPS code ship and company-related costs

110. Summarising the previous two sections on ISPS Code-related ship and company costs, we estimate the initial ISPS Code compliance burden on ship operators to be *at least* ~USD 1 279 million and USD 730 million per year thereafter. Not included in these estimates are the costs of implementing IMO AIS requirements (since these were only accelerated by the MSC 76 SOLAS modifications) and the indirect costs of operating under level 2 and 3 security alerts (potentially very large) . The addition of the latter two into these estimates would possibly change the order of magnitude of costs under consideration.

111. As can be seen from the figure below, the bulk of costs faced by ship owners/operators are related to creating a new Company Security Officer post and to equipping their vessels with security-related equipment . Security staff costs also form the majority of recurring security-related costs as maintenance costs for security equipment are relatively low. Given the relative size of security staff costs in overall security expenditures, it is possible that a greater number of "large" companies than we have assumed for this exercise will seek to assign Company Security Officer Responsibilities to an existing staff position.

Distribution of SOLAS/ISPS Code Ship and Company-related Costs*



* Not included in these estimates are the costs of implementing IMO AIS requirements and the indirect costs of operating under level 2 and 3 security alerts (potentially very large).

Measures targeting ports

112. Chapter X1-2 of SOLAS and the ISPS Code set out broadly analogous requirements for ports as they do for vessels. Ports facilities that receive vessels engaged in international trade are required to:

- Carry out, and have approved, port facility security assessments.
- Develop port facility security plans that detail measures to be taken at each security alert level, and address single-ship security alerts.
- Designate a Port Facility Security Officer (PFSO) with skills and training roughly similar to the CSO.
- Ensure that the PFSO and other appropriate personnel receive adequate training to carry out their duties and that security drills are held to ensure the readiness.
- Ensure that port facilities are sufficiently equipped and staffed in order to operate under the three security alert levels.

113. Assessing the port-related costs of the ISPS Code is complicated by the great number of ports world-wide and their diversity. The United States Department of Transport identifies at least 3 970 ports in the world (USDOT listing of world ports in "schedule K"). However, a quick assessment of these reveals that some of these ports are only very marginally involved in international trade. Fairplay/Lloyd's Register count 2 814 port authorities world-wide. For the purposes of this report, we will assume the latter to be representative of the universe of ports involved in international trade. These range from megaport complexes that house numerous berths, terminals and facilities to small, single-berth ports that are only infrequently involved in international trade. Furthermore, these port facilities range from highly automated modern container facilities to oil terminals, dry bulk facilities and multiple-use berths. The potential costs faced by port facilities can also vary by several orders of magnitude according to local labour costs, port characteristics and port size.

114. The ISPS Code targets *port facilities*; however data on the number of port facilities (private berthing quays, independent terminals, etc.) within the world's 2 814 international cargo ports is hard to come by. To give an idea of the discrepancy between ports and the port facilities they contain, the United States counts *226 ports* and *4 365* port facilities. The Fairplay's/Lloyd's List World Ports and Terminals Guide lists approximately 6 500 port facilities. While this figure is only a third larger than the number of American port facilities as counted by the American Coast Guard, it should be noted that the latter include many domestic-only facilities along inland waterways and in the Great Lakes area. Furthermore, the United States are home to several large multiple-terminal ports such as the Port of Houston, the Port of South Louisiana, and the container ports of Los Angeles/Long Beach and New York. This may partly account for the high number of American port facilities. We will therefore adopt the Fairply/Lloyd's List figure 6 500 port facilities as a conservative estimate of the number of facilities worldwide.

115. United States Coast Guard cost estimates for United States port facility compliance with the ISPS code will serve as a basis for our cost calculations. However we will opt not to include certain expenditure categories and ports where data is lacking on local costs, and where it is unreasonable to project USCG estimates. This means that the focus of the section below will necessarily focus on the world's top ports.

Port facility security assessment

116. As with individual ships, the ISPS Code mandates that port facilities undertake comprehensive security assessments that, at a minimum, cover the following four items:

- Identification and evaluation of important assets and infrastructure it is important to protect.
- Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures.
- Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability.
- Identification of weaknesses, including human factors in the infrastructure, policies and procedures.

117. The cost of undertaking a Port Facility Security Assessment will likely vary among ports according to their size and desire to go beyond minimal compliance with the new IMO security rules.

118. The world's top 40 ports (by tonnage) accounted for approximately 80% of total international seaborne trade by goods loaded in 2000. The corresponding figure for TEU's handled by the top 40 container ports was 63% in 2001. We assume that these ports are global competitors and will seek a high standard of compliance with the ISPS Code. These port facilities will therefore face higher PFSA costs. We will further assume that these ports contain a higher share of port facilities than other ports – these ports represent 1.5% of ports worldwide and we will assume that they represent 7.5 % of port facilities. The USCG estimates PFSA costs for high-standard port facilities to be USD 8 000 initially and USD 400 per year thereafter. Corresponding costs for lower-standard port facilities are USD 4 000 and USD 100, respectively. Thus we estimate the costs of undertaking Port facility Security Assessments for the world's international cargo port facilities to be approximately USD 27.9 million initially and approximately USD .8 million annually.

- Direct costs: ~USD 27.9 million Yearly maintenance costs: ~USD .8 million

Port facility security plan

119. Like its ship-related counterpart, the Port Facility Security Plan must be based on the outcome of the Port facility security Assessment and must take into account the following 15 elements:

- Measures designed to prevent weapons or any other dangerous substances and devices intended for use against people, ships or ports and the carriage of which is not authorized, from being introduced into the port facility or on board a ship.
- Measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility.
- Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface.
- Procedures for responding to any security instructions the Contracting Government, in whose territory the port facility is located, may give at security level 3.
- Procedures for evacuation in case of security threats or breaches of security.
- Duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects.
- Procedures for interfacing with ship security activities.
- Procedures for the periodic review of the plan and updating.
- Procedures for reporting security incidents.

- Identification of the port facility security officer including 24-hour contact details.
- Measures to ensure the security of the information contained in the plan.
- Measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility.
- Procedures for auditing the port facility security plan.
- Procedures for responding in case the ship security alert system of a ship at the port facility has been activated.
- Procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship including representatives of seafarers' welfare and labor organizations.

120. As with the PFSA, the PFSP will likely involve varying costs according to port facility size, operations, etc. The USCG considers the costs of elaborating the PFSP to be roughly analogous to the cost of undertaking a PFSP. Therefore we estimate the costs for developing PFSP for the world's cargo port facilities to be USD 27.9 million initially and approximately USD .8 million annually.

- Direct costs: ~USD 27.9 million Yearly maintenance costs: ~USD 8 million

Port facility security officer, port facility security training and drills and port facility security equipment and staffing costs

121. Port facilities are required to designate a Port facility Security Officer responsible for one, or several, port facilities. The PFSOs must possess specific security-related skills and must be trained in order to fulfil their roles which must include the following 13 responsibilities:

- Conducting an initial comprehensive security survey of the port facility taking into account the relevant port facility security assessment.
- Ensuring the development and maintenance of the port facility security plan.
- Implementing and exercising the port facility security plan.
- Undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures.
- Recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility.
- Enhancing security awareness and vigilance of the port facility personnel.
- Ensuring adequate training has been provided to personnel responsible for the security of the port facility.
- Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility.
- Coordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s).
- Coordinating with security services, as appropriate.

- Ensuring that standards for personnel responsible for security of the port facility are met.
- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.
- Assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

122. It is too early to attempt to estimate what cost will be entailed by the deployment of Port facility Security Officers in 2 810 ports and twice as many facilities in 131 countries around the world.

123. The first difficulty lies in the fact that PFSO's can be assigned to one or several facilities and it is unclear how many PFSO's will be responsible for multiple facilities. The second difficulty is that PFSO responsibilities might be assigned to a new post by the port facility operator or folded into an existing post. The USCG estimates that 1/3 of American Port facilities will create a dedicated PFSO position, while the remainder will likely add PFSO responsibilities as a ½- or ¼ -time post, according to facility type.

124. The second and perhaps greatest difficulty in estimating the burden imposed by the PFSO requirement is that there are no data on international labour costs for these officers. PFSO's will in some cases be national government positions, regional/local government positions or private sector positions. Furthermore, even among private sector facility operators there are vast differences in pay between local and multi-national terminal operators. Furthermore background requirements, and corresponding labour rates, for PFSO's will change from country to country. Even though the very top port facility operators are likely to be operating in roughly the same labour market for their key management executives, we cannot say with certainty whether the pool of such ports is confined to the top 5 the top ten or any other subset of the world's top-ranked ports.

125. For these reasons, it is premature to attempt to gauge the labour costs associated with the new Port Facility Security Officer position.

126. Other port requirements in the ISPS cover training needs for PFSO and other appropriate staff (*e.g.* security officers, security drills, and equipment/staff expenditures necessary to adequately carry out the Port facility's Security Plan. Again, estimating the costs of these investments is an extremely complicated task given the great variability of costs from port to port. Hourly labour wages for security guards vary from just slightly higher than day-labourer levels in many areas (*e.g.* Africa, South-west Asia) to relatively high government pay levels. Costs for equipment (fencing, lighting, secured gates, locks, communications equipment, monitoring equipment, etc) also vary tremendously according to local construction and installation-related labour costs and port size and equipment needs. Finally, many ports, in order to reduce losses from cargo theft, have already invested heavily in security infrastructure and equipment. For all of these reasons, we cannot estimate with any level of certainty what the cost impact will be from the ISPS requirements for PFSO training, security staff training, port security drills, port security equipment investments implied by PFSP's and additional labour costs generated by new security guards required to implement PFSP's.

127. However, in order to give an idea of the scope of costs likely to be faced for the expenditures outlined above, we can turn to the USCG's estimates of these costs for the United States. In order to account port's past investments in security equipment, guards, etc, the USCG estimated the percentage of port facilities that would require new investments in order to comply with the United States Maritime Security Act of 2002 which translates the IMO ISPS Code into national legislation. As seen from the table below, a number of facilities already have sufficient security equipment/guards in place – especially among terminals handling hazardous cargoes and containers. The fact that American bulk cargo terminals will

require greater ISPS-related investments will likely be mirrored at the international level given that these terminals have generally been less concerned with cargo theft losses.

Estimated Percentage of American Port Facilities that will Purchase/Enhance Security measures by Facility Type					
	Container, Break-bulk	Dry Bulk	Hazardous Bulk Liquid	Other Hazardous Cargo	Other Bulk Liquid
Hand-held radio	5	70	5	5	10
Gates	30	70	10	5	10
CCTV	5	10	5	5	10
Lights	5	60	5	5	10
Com. System	5	0	5	5	10
Fencing	5	20	5	5	10
Security Guards	30	70	10	5	10

128. These costs represent 61% of the first-year burden of United States Port Facilities' compliance with the ISPS Code (see table below) and 37% of the annual cost of ISPS compliance by Port facilities. These ratios are likely not to be duplicated internationally because the labour costs associated with the PFSO and security guard positions are significantly higher in the United States than in many other countries. What can be concluded from the table below is that annual ISPS Code compliance costs for international port facilities are likely to be dominated by PFSO and security guard labour costs just as they are in the United States.

American Initial and Annual ISPS Code Compliance Costs by Category (million USD)				
Category	Initial Cost	*Percent of Total*	Annual Cost	*Percent of Total*
Port Facility Security Assessment	23	*2*	1	*0*
Port Facility Security Plan	23	*2*	1	*0*
Port Facility Security Officer	335	*35*	335	*63*
Security Training	17	*2*	17	*3*
Port facility Security Drills	0	*0*	35	*7*
Security Guards	124	*13*	124	*23*
Security Equipment	441	*46*	22	*4*
Total	**963**	*100*	**509**	*100*

- Direct costs: undetermined Yearly costs: undetermined (dominated by labour costs)

Non-IMO mandatory measures

United States Maritime Transportation Security Act of 2002

129. In reaction to increased calls for greater maritime transport security measures, the United States Senate and House passed public law 107-295 – the American Maritime Transportation Security Act of 2002 – in November of 2002. The bulk of the maritime-security related provisions of the law are in its first section and mainly serve to enact into American law the security-related modifications of SOLAS and the ISPS Code. The USCG has estimated the American compliance cost for the SOLAS- and ISPS Code-related provisions of the law to be approximately USD 1.2 billion initially and approximately USD 699 million every year thereafter. For the next 10 years, the USCG estimates the present value of these expenditures (7% discount rate) to be approximately USD 5.97 billion – largely dominated by port-related costs (USD 1.1 billion for vessel security and USD 4.87 billion for port security).

130. The Maritime Transportation Security Act also includes several new measures that go beyond what has been agreed at the IMO. Among these are requirements for "Transportation Security Cards" for port personnel, new secure seafarer identification papers (if these are not agreed-upon through negotiations at the International Labour Organization within 2 years) and the development of a system of foreign port security assessments.

131. It is the latter – the requirement to assess security plans and procedures at foreign ports -- that has the greatest potential to impose significant costs. While standards for these assessments have not yet been promulgated, the law does allow for the United States to bar access to its ports for vessels arriving from what it will consider to be "unsafe" ports Under the new IMO rules, Port States are ultimately be responsible for validating the PFSA's and PFSP's that should guarantee (at least nominally) a certain level of security. The American law would further allow the United States to make a judgement on the effectiveness of the foreign Port State's oversight. The extent of costs associated with this clause will depend on the number of non-American ports "blacklisted", their volume of trade and the measures taken by American authorities to counter what they perceive as the security threat posed by shipments from these ports (*e.g.* greater cargo scrutiny, full cargo screening, outright ban on arrival of the vessel in the United States, etc.). It is still too early to attempt to estimate these costs.

United States 96-hour advance notification of arrival

132. On 4 October 2001, the USCG issued a modification to its notification of vessel arrival requirements for United States ports. Whereas previously, vessels were required to provide notice of their arrival 24 hours ahead of their scheduled arrival time, the new rule quadrupled this requirement to 96 hours. Following two subsequent amendments to the temporary rule, the USCG issued a final rule on 28 February 2003. The final rule upheld the 96-hour advance notification requirement and added further requirements regarding the submission of cargo manifests, itinerary and extensive crew information including ports where crew boarded and possible aliases crew are known to employ.

133. Ship operators have generally not objected to the central thrust of the new notification of arrival rules, but have pointed out that some of the detailed provisions of the rule will be problematic to enforce (*e.g.* the provision of crew "aliases"). Furthermore, they have expressed some concern regarding duplicative data submission requirements (*e.g.* crew information to be supplied to the USCG and immigration authorities, Cargo manifests to be supplied both to the USCG and to the American Customs Service). Finally, the cargo manifest filing requirement involves some data processing time and software costs given the USCG's preference to see this information submitted electronically. Overall, however,

compliance costs for this rule should not be too significant. Absent better data from ship operators, we will use the USCG's estimate of approximately USD 6.7 million per year.

- Annual costs: ~USD 6.7 million/yr

Department of State crew visa requirements (proposed)

134. On December 13, 2002, the United States Department of State issued a proposed rule -- The Enhanced Border Security and Visa Entry Reform Act of 2002 – to discontinue the use of crew list visas and require foreign seafarers to individually apply for non-immigrant visas in order to accommodate new requirements for biometric indicators on visa forms. .Crew list visas are typically used to expedite the entry process for workers such as seafarers and air crews whose work brings them temporarily to a foreign country. Given that 6 353 vessels visited American ports in 2000 and assuming an average crew size of 15-20, we estimate that approximately 95 000-127 000 seafarers visited the United States in that year. While some of these seafarers are American citizens and are therefore exempt from the proposed visa requirements, the overwhelming majority are foreign nationals. Crew list visas used to be fairly inexpensive (approximately USD 45 per visa) but the proposed change in visa requirements and the recent, unrelated increases in the cost of processing crew list visas (from USD 45/seafarer to USD 100/seafarer in November 2002) will have important repercussions for ship-operators visiting the United States. Direct visa-related fees could range from USD 95-127 million to which additional costs (*e.g.* interview requirements, cost of intermediaries, etc) must also be added.

135. Other crew-visa related costs have to do with differing local federal agencies' interpretation of seafarer visa requirements. Seafarers lacking proper individual visas, lacking proper identification documents, missing from crew list visas and/or simply being nationals of certain countries having certain nationalities have been prevented from disembarking in many American ports. Data collecting from the American-based Center for Seafarer Rights in early 2003 show some major American ports experiencing denial of shore leave incidents for as many as 40% to 64% of all visiting vessels during the period covered. In some cases (*e.g.* for some oil and gas terminals), all seafarers irrespective of their visa status have been detained on board. In many of these cases, armed security guards have been posted at the owner's expense.

136. The United States Immigration and Naturalization Service (INS) keeps a "watch list" of nations whose visa applications receive greater scrutiny from its officials. This list is classified but a certain number of countries, including Malaysia, Pakistan, Indonesia and nations with a suspected presence of Al'Qaeda operatives are known to be on the list. Given the activities of the Al'Qaeda-linked Philippine-based Abu-Sayef terrorist group, it is not unreasonable to imagine that the Philippines, the world's largest supplier of seafarers (~20% of the world's seafarers), might also figure on that list. In addition to the Philippines, Intertanko has identified a number of other nationalities that seem to trigger greater scrutiny from United States immigration officials including Turkey, Russia and the Ukraine. Collectively these countries represent approximately 40% of the world supply of all seafarers. Were American visa applications from seafarers of these nationalities processed more slowly and/or blocked, the world trading fleet would experience great difficulty operating its vessels in the United States.

Top Ten Labor-Supplying Countries (2000)		
Country	Officers	Ratings
China	34 197	47 820
Greece	17 000	15 500
India	11 700	43 000
Indonesia	15 500	68 000
Italy	9 500	14 000
Japan	18 813	12 200
Philippines	50 000	180 000
Russian Federation	21 680	34 000
Turkey	14 303	48 144
Ukraine	14 000	23 000
Total Supply of Ratings from the Top Ten suppliers	206 693	485 664
Total Supply of Seafarers	1 227 000	

Source: BIMCO/ISF manpower update, 2000, and Couper *et. al*, 1999.

137. As outlined in this section, the proposed new American seafarer visa requirements have the potential to impose significant burdens on vessel operators visiting the United States. However, because these rules have not yet been finalised, and it is unclear at the moment of this report's writing to what extent they will remain unchanged, it is premature to estimate their total cost burden.

United States 24-hour advance manifest rule

138. This unilateral measure imposed by the United States for containers loaded onto vessels destined for its ports is probably the most contentious of all of the security measures announced to date. Succinctly, the rule obliges carriers and/or non-vessel operating common carriers (NVOCCs -- freight forwarders acting as principal transport agents) with automated data submission capabilities to submit a cargo declaration 24 hours before a container is to be *loaded* on board a vessel bound for the United States. The rule is applicable both to containers to be discharged in the American as well as containers loaded on the vessel for non- American destinations, but does not apply to empty containers.

139. The rule is a response to the risk for containers to be used to transport weapons of mass destruction. Because these weapons might target ports in the United States, the rule's premise is that security assessments of containers should be undertaken *before* containers are loaded onto a ship and are underway. Indeed container inspections are extremely difficult to carry out on board a modern container vessel where the majority of the containers may be inaccessible below deck.

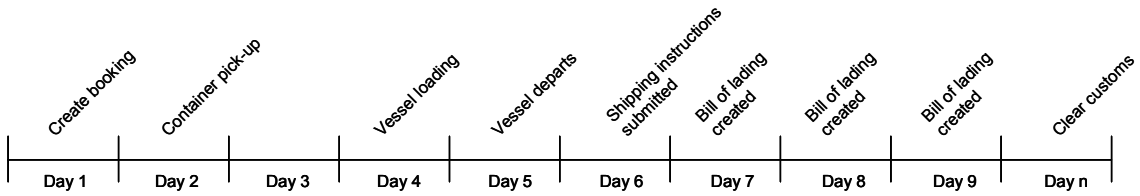
140. Based on the manifest data (consignor, consignee intermediaries, origin port, description, count, etc.), American Customs applies 55 rules in an automatic profiling system. These rules are not made public but some manifest data will automatically give containers a high targeting score and others will fail the container outright. Among the former are masked shipper or consignee information (including post box

address) and certain countries of origin for either the goods or the shipment. Included in the latter are imprecise descriptions of the container's contents such as the widely-used "said to contain", "FAK" (freight all kinds)", general merchandise", etc. After inspecting the manifest data, American Customs makes a decision to allow the carrier to load the container or to issue a "do not load" message to the port authority before the container's scheduled load time. In the latter case, the port authority notifies the carrier and the container is not allowed to load. If a carrier loads a "do not load" container, the vessel will not be allowed to discharge at an American port.

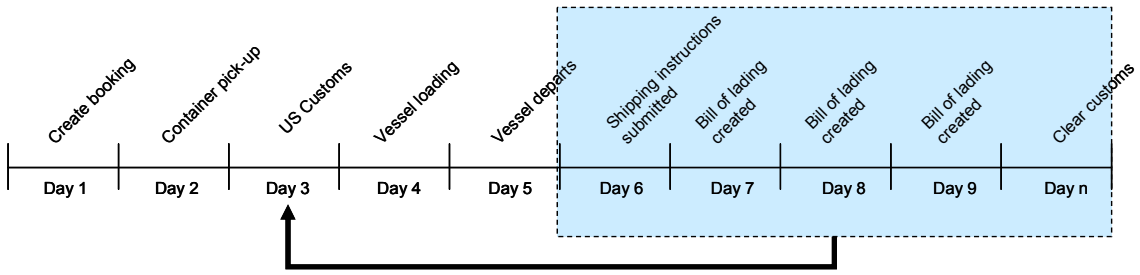
141. The 24-hour rule became effective on December 2, 2002. However, in order to give importers a "breaking-in" period, American Customs declared a 60-day non-enforcement period during which non-fraudulent violations would not trigger the rule's provisions, including penalties. The rule became fully effective and enforced on February 2, 2003.

142. The new requirements of the 24-hour rule break significantly with past practice in the maritime transport sector. Previous to the 24-hour rule, American Customs would accept final bill of lading information up to 30 days *after* a shipment's arrival in the United States. This relatively long time-lapse suited most carriers well since booking container space on a vessel remains a slow manual process (with the exception of some large shippers and forwarders). In many cases, the process of manually re-entering bill of lading data provided by the shipper only commences once the vessel is already underway.

Typical Container Booking/Bill of Lading Cycle: before 24-hour advance notification



Typical Container Booking/Bill of Lading Cycle: after 24-hour advance notification



143. The principal impact of the 24-rule has been to move up the later steps in the booking cycle to 24-hours *before* the container is loading on board the ship. This imposes costs on carriers who must field sufficient clerical/data entry staff to handle bookings 24 hours a day and seven days a week. Some carriers have also expressed fears that the rule would reduce their flexibility to accept last-minute bookings although only the *time* at which they can accept last-minute bookings has changed. Finally carriers have expressed concern that the new requirements – and the carriers' liability under these requirements (*e.g.* for the proper and accurate description of the contents of containers they have not packed) – may have significant impacts in the event of loss, theft or terrorist attack.

144. Shippers have also expressed concerns regarding the costs stemming from the early manifest requirements. Among these are the costs associated with paying for port space for containers shipped in advance of the 24-hour deadline. While the rule states that only data regarding the shipment must be provided in advance of loading, a recent survey shows that 15% of shippers are also providing their loaded containers early. In some congested ports, this influx of containers needing temporary storage has also entailed costs. The same survey found that 30% of shippers are building buffer periods in their logistics operations to account for the rule. This buffer period often extends beyond the 24-hour period given that some carriers are requiring shippers to provide data even earlier so that they have time to re-key and transmit the data to American Customs.

145. All of the above factors have led some analysts to predict that the overall cost of the 24-hour rule will be in the order of USD 5-10 billion per year[8]. However, at the time of this report's writing, the rule has only been enforced for 2 months and there is only scant evidence as to the actual costs of this rule. Despite strong and vocal concerns regarding shipper non-compliance with the rule, experiences have been largely positive so far. In the first week of compliance enforcement, American Customs issued 13 "no-load" orders among 143 000 bills of lading (although Customs has admitted it principally focused compliance with cargo designation terminology – a broader focus may have resulted in more containers held). In fact, many shippers have pointed to benefits from the rule stemming from the tighter control of supply chains. The only tangible cost data emerging from implementation of the rule has been from forwarders and carriers themselves.

146. In response to mostly staff costs associated with the new 24-hour rule requirements, several carriers and forwarders have introduced new "documentation fees" into their container rates. These are detailed below. Assuming that a) these fees accurately reflect carrier costs (which some shippers dispute) and b) all carriers importing containers to the United States face these same costs, we can get a general idea of the potential burden imposed on carriers by the rule – approximately USD 281.7 million/yr (11 268 000 TEU's imported by sea in 2001 multiplied by USD 25).

[8] "Ten billion dollar costs for 24-hour rule", CI-Online (www.ci-online.co.uk), 12 March, 2003.

Name	Activity	Basis	Base fee (USD)	Corrections fee
Danzas	Forwarder	Container	25	
Panalpina	Forwarder	Bill of Lading	40-60	
Kuehne & Nagel	Forwarder	Bill of Lading	35	
OOCL*	Carrier	Bill of Lading	25	40
Maersk Sealand*	Carrier	Bill of Lading	25	40
P&O Nedlloyd*	Carrier	Bill of Lading	25	40
APL*	Carrier	Bill of Lading	25	40
Hapag-Lloyd*	Carrier	Bill of Lading	25	40
CMA CGM*	Carrier	Bill of Lading	25	40
Cosco*	Carrier	Bill of Lading	25	40
HMM*	Carrier	Bill of Lading	25	40
K Line*	Carrier	Bill of Lading	25	40
MOL*	Carrier	Bill of Lading	25	40
NYK Line*	Carrier	Bill of Lading	25	40
Yangming*	Carrier	Bill of Lading	25	40
Hanjin*	Carrier	Bill of Lading	25	40
Evergreen*	Carrier	Bill of Lading	25	40
Shipping Corporation of India	Carrier	Container	25	
Contship Containerlines	Carrier	Container	25	
CSCL	Carrier	Bill of Lading	25	

* members of the Transpacific Stabilisation Agreement

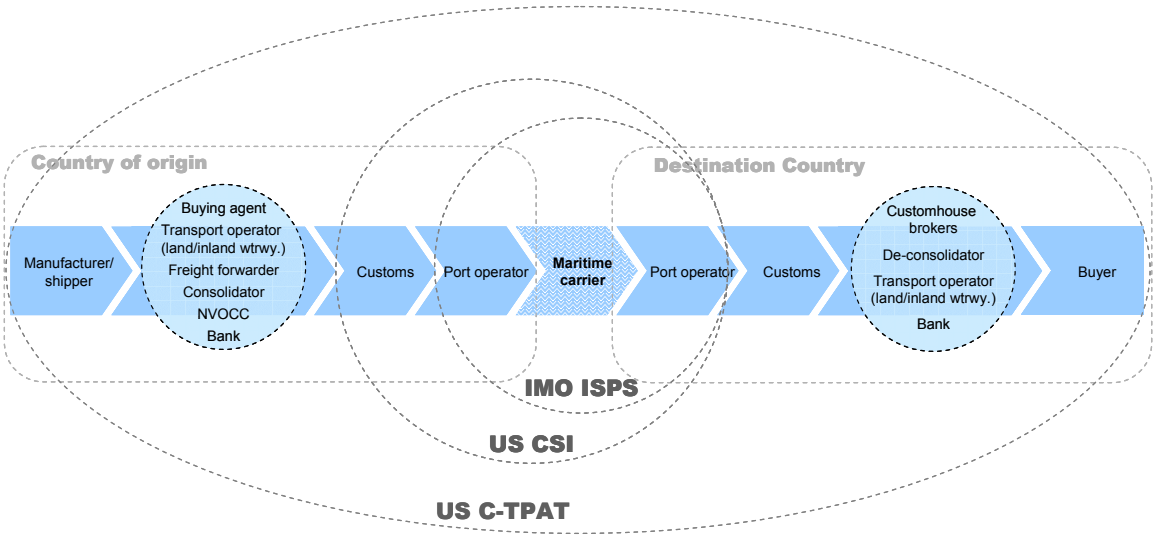
- Annual costs: unknown (USD 281.7 million/yr – USD 10 billion/yr)

Voluntary measures: United States

147. Voluntary programmes are by their nature non-binding and the costs resulting from participation in these programmes are not part of the regulatory burden faced by the actors in the maritime sector. However, this does not mean that these programmes do not sometimes have indirect costs that can be very real. We will examine two voluntary maritime security initiatives proposed by the United States and examine some of the economic ramifications of these. These programmes are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT).

148. Both of these programmes share the same premise as the mandatory 24-hour Advance manifest Rule – namely that given the risk that containers pose once they reach a destination port, it is preferable to ensure their contents and integrity as far upstream in the logistics chain as possible. Thus CSI moves the loci of container inspection into origin ports and C-TPAT moves the loci of ensuring container integrity all the way to the origin shipper.

International Container Logistics Chain Vulnerability Assessment:
Scope of IMO and US Security Initiatives



Container Security Initiative (CSI)

149. The Container Security Initiative seeks to develop bi-lateral agreements between the United States and foreign countries to pre-screen high-risk containers in ports of loading. The vast majority of containers do not pose any security threat. All identified high-risk containers will be inspected, either before loading at a CSI port or, if arriving from another port, upon arrival in the United States. In CSI ports, local customs officials and a team from the U.S. Bureau of Customs and Border Protection will decide on which containers to inspect before loading.

150. The initiative is built around 4 principal elements:

- Establish security criteria to identify high-risk containers.
- Pre-screen those containers prior to American arrival (involves the deployment of American Customs officials to foreign ports).
- Use technological means to pre-screen these containers.
- Develop and use IT-enabled and secure containers.

151. As of June 2003, 23 ports representing at least 60 % of container imports to the United States had signed CSI agreements and the CSI was operational in 15 of these (Antwerp, Bremerhaven, Felixtowe, Genoa, Göteborg, Halifax, Hamburg, le Havre, Hong Kong, Montreal, Rotterdam, Singapore, la Spezia, Vancouver and Yokohama). The direct costs of participation include the purchase/upgrade of container scanning systems if existing container scanning capacity is not sufficient. Container scanners can cost between USD 1-5 million and can handle anywhere from 4-20 containers per hour according to the technology employed. Depending on the nature of port management and national Customs arrangements, these costs can be borne by any number of parties ranging from national governments, local port authorities (government or private) and commercial terminal operators. Furthermore, any of the previously mentioned parties may, or may not, put in place cost-recovery mechanisms such as container surcharges, scanning fees, port duties, etc.

152. Scanning high-risk containers also generates indirect costs linked to the number of container yard moves and time required to get the container out of a stack, to the scanning station, and back. These costs, again, are variable depending on such factors as port size and layout, local labour rates and container yard technology.

153. American Customs has not yet determined what standards to apply to meet the definition of "smart and secure" containers. There are many competing technologies available ranging from off-the-shelf systems to untested experimental technologies. Costs associated with these vary tremendously as well and currently do not represent savings that would become available with greater economies of scale. As such, we feel it is still too early to estimate what "Smart and Secure" containers will cost – except to say that it will be more than current container costs.

Top 20 Container Ports Exporting to the United States and CSI Participation: March 2003		
Port	% of American Container Imports	CSI Status
1. Hong Kong	9.8	Yes
2. Shanghai	5.8	Yes
3. Singapore	5.8	Yes
4. Kaohsiung	5.6	
5. Rotterdam	5.1	Yes
6. Pusan	5.0	Yes
7. Bremerhaven	4.5	Yes
8. Tokyo	2.8	Yes
9. Genoa	2.1	Yes
10. Yantian	2.0	Yes
11. Antwerp	2.0	Yes
12. Nagoya	1.9	Yes
13. Le Havre	1.9	Yes
14. Hamburg	1.8	yes
15. La Spezia	1.7	yes
16. Felixstowe	1.7	yes
17. Algeciras	1.6	yes
18. Kobe	1.6	yes
19. Yokohama	1.5	yes
20. Laem Chabang	1.4	yes
Other ports in CSI		
Gothenburg		
Klang		
Colombo		
Tanjung Pelepas		

Customs-Trade Partnership against Terrorism (C-TPAT)

154. C-TPAT is the second major voluntary supply chain security initiative announce by the United States. It aims to ensure that participants implement policies, plans and procedures to ensure the integrity of their entire supply chain. Specifically, participants must sign an agreement that commits them to the following four actions:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. These guidelines encompass the following areas: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security.
- Submit a supply chain security profile questionnaire to Customs.
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

155. In return, once American Customs have validated the participant's plans, C-TPAT participants are less likely to be targeted for customs inspections and benefit from expedited customs procedures.

156. The potential costs to participants are great as they must invest in securing the physical integrity of their own premises, but also ensure that their trading partners do so as well. Other costs include training staff, adding security guards, developing plans and processing C-TPAT paperwork. Although C-TPAT participation will require substantial investments for some shippers, intermediaries and carriers, others already have in place fairly strong security practices that were originally put in place to counter the risk of theft. The latter will likely face lower participation costs.

Impacts on competition

157. Possibly the greatest potential cost of both CSI and C-TPAT have to do with the competitive advantage that participants could derive over others. Indeed non-participants in both programmes face greater scrutiny and delays when shipping to the United States. The threat of differential treatment between CSI and non-CSI ports has been one of the principal factors behind the number of ports signing up to the programme. Likewise, large shippers have been quick to seek C-TPAT validation in order to expedite their American-bound shipments. Smaller ports and some small shippers have complained saying that they simply cannot afford to compete with CSI and C-TPAT participants and that their shipments will be penalised through their non-participation. This may be true, but it must be pointed out that while these programmes might have impacts on intra-port and intra-shipper competition, they do not bring about *unfair* competition. Participants are simply investing in greater security, a premium which the United States is willing to "pay" for through expedited cargo processing.

6. CONCLUSIONS

158. The Al'Qaeda attacks on the World Trade Center represented perhaps the first incidence of mega-terrorism. The success, with which Al'Qaeda mobilised resources, planted and trained operatives over a two-year period across several countries and planned, co-ordinated and carried out four near-simultaneous attacks on the territory of the world's largest superpower ushered in a sobering new era. What before had been taken for granted, suddenly became a source of worry – and the world maritime transport system proved to be no exception.

159. This system, moving billions of tons of goods and millions of containers on thousands of vessels operated by hundreds of thousands of seafarers between thousands of world ports, has been predicated on two principles – open participation and the unfettered flow of trade. These principles allowed the maritime transport network to deliver tremendous gains in prosperity, and yet now -- following the September 11th attacks – has become a source of alarm for world governments.

Maritime transport is open… and vulnerable

160. The maritime transport system is vulnerable to being used and/or targeted by terrorists. It is vulnerable because the system is largely open and porous enough that terrorists can enter and/or manipulate it according to their purposes. This is especially true of the container transport system where the velocity of trade, the use of anonymous and uniform containers and the relative ease with which the contents of the latter can be wilfully misrepresented, offer many opportunities for terrorists – just as they currently do for drug and contraband smugglers. Bulk shipments also pose a danger because of the dangerous nature of some of their cargos.

161. The system is already targeted by pirates and criminals with some success in various parts of the world and seafarers often bear the brunt of these attacks. But some seafarers themselves, or people posing as such, are implicated in some acts of piracy, just as some port workers are implicated in cargo theft. We cannot assume that terrorists have not noticed these stratagems and are not already planning to adapt them for their purposes.

162. Finally, the maritime transport sector, largely because of the availability of opaque ownership disclosure requirements (or lack thereof), can provide an attractive option for groups seeking to combine legitimate "front" revenue-generating businesses with a more sinister global logistics.

Disruption of maritime trade bears tremendous potential costs

163. The economic impact of a terrorist attack using, or targeting, maritime transport is difficult to gauge. What is clear is that the direct impact of such an attack would be several orders of magnitude smaller than the potential indirect impacts caused by a disruption in world trade and the cost burden of emergency security measures. These costs could be as high as USD 58 billion, for the United States alone, following an orchestrated campaign of terror. Any loss-causing disruption in world trade would also have a relatively larger impact on many developing countries whose economies are more export-dependent.

Finally adaptive strategies by businesses in the face of such risks, such as increases in inventory holdings can go far to wipe out recent gains in supply-chain performance and logistics savings.

International and national security measures reduce this vulnerability… at a price

164. Measures addressing the most obvious gaps in maritime security have been negotiated and approved at the IMO or have been initiated by the United States. Many of these measures have yet to come into force and for those that are currently effective (03/2003) scant evidence exists on their costs. We have attempted to estimate those costs that can be quantified and have sought to speak to the cost considerations of other measures for which data is currently lacking. These costs are tabulated below according to the measure in question, its initial, yearly and possible indirect costs, our confidence level with the estimate provided, and an assessment of the non-antiterrorism benefits that might result from implementation of the measure.

165. As indicated in the paper and summarised below, IMO measures targeting companies and ships share a higher overall confidence rating than other IMO measures targeting ports and many of the American initiatives. We estimate the initial ISPS Code compliance burden on ship operators to be *at least* ~USD1 279 million and ~USD 730 million per year thereafter. However, costs stemming from implementation of the ISPS Code for port facilities are likely to be as large if not larger.

166. We have less overall confidence in our judgement of costs stemming from many of the American initiatives simply because these have fewer technical elements and have a potentially broader and more diffuse effect. What can be said is that for many of the costs where we have a reasonable level of confidence, we are dealing with sums that are many orders of magnitude smaller than those that might result from a trade-disrupting terrorist attack.

Summary Table: Costs of Maritime Security Measures and Assessment of non Anti-terrorism Benefits					
Measure	Initial Cost - approximate (million USD)	Yearly Cost - approximate (million USD)	Indirect Costs	Confidence level	Non-terrorism Benefits
IMO SOLAS/ISPS Code					
Government Security Alert Levels	(low)	n/a	potentially large	low	+
Automatic Identification Systems	649.3	(undetermined)	undetermined	high	+++
Ship Security Alert System	86.5	4.3	0	high	
Ship Identification Number	21.6	n/a	0	medium	+
Company Security Officer (large companies)	514.6	514.6	undetermined	medium	+
Company Security Officer (small companies)	150	150	undetermined	low	+
Ship Security Assessment	103.9	(low)	0	medium	
Ship Security Plan	51.9	(low)	0	medium	

Ship Security Officer	29	29	0	medium	+
Ship Security Training/drills	16.8	16.8	0	medium	
Vessel Security Equipment	304.4	15.2	0	high	+
Record-keeping	(low)	(low)	0	high	
Port facility Security Assessment	27.9	.8	0	low	++
Port facility Security Plan	27.9	.8	0	low	++
Port facility Security Officer	(undetermined)	(undetermined)	(undetermined)		++
Port facility Training/drills	(undetermined)	(undetermined)	(undetermined)		+
Port facility Security Equipment/staff	(undetermined)	(undetermined)	(undetermined)		+++
United States Maritime Security measures					
Maritime Transportation Safety Act of 2002 (non-IMO provisions)	(undetermined)	(potentially large)	(undetermined)		
96-hour Advance Notification of Arrival	6.7	6.7	(undetermined)	high	
INS Crew Seafarer Requirements (proposed)	95 (at least)	(undetermined)	(high)	low	
24-Hour Advance Manifest Rule	281.7 to 10 000	281.7 to 10 000	(undetermined)	low	++
Container Security Initiative	(undetermined)	(undetermined)	(undetermined)		+
Customs-Trade Partnership against Terrorism	(undetermined)	(undetermined)	(undetermined)		+++

The silver lining…security costs versus trade benefits

167. This paper has examined the maritime transport system's vulnerability to terrorism, and sought to gauge the cost of measures proposed to remedy the most flagrant gaps in security. It should be pointed out, however, that many of the measures proposed have distinct *benefits* that are not related to their anti-terrorism task. These benefits result from reduced delays, faster processing times, better asset control, decreased payroll (due to IT improvements), fewer losses due to theft, decreased insurance costs, etc. While some measures may slow trade, many others can in fact lower trade costs.

168. In an industry still largely dependent on paper and fax transmissions, it is not hard to see room for savings resulting from more integrated IT systems. Many large manufacturers/shippers have already benefited from increased productivity due to IT improvements in their supply chain. If these were extended to all trading parties – small shippers, forwarders, land and sea carriers, customs authorities, port and terminal operators, etc. – the savings could be tremendous. Vessel turn-around times could be shortened,

customs clearing accelerated and costs associated with redundant data entry eliminated and cargo handling costs slashed[9].

169. While the calculation of these benefits falls beyond the scope of this report, some insight may be gained by looking at non-security inspired projects that may have similar impacts on trade facilitation. For example, cost-benefit analyses of a new electronic customs manifest handling system proposed by American Customs before September 11th, 2001 the Automated Commercial Environment – ACE), estimate the direct savings to American importers alone to be USD 22.2 billion over 20 years and the American government savings to be USD 4.4 billion over the same period. While these estimates are not directly transposable to security-related measures, they do provide a glimpse of the type of savings that can be realised as a result of faster processing times, better asset control, reduced theft, etc. – all potential benefits of the new maritime security measures.

170. In the end, most participants in the international maritime trading system agree that the recently enacted maritime security measures are desirable. They are not free, but they do bring about benefits that go beyond their mitigating impacts on terrorism. The extent of their costs is uncertain but is likely to be much less than the extent of costs linked to inaction. What is certain is that some of these measures have the potential to change long-established practices in the industry – for the better. This then, is the silver lining. Responses to terrorist threats to the sector have offered new opportunities for the maritime transport industry to better organise itself, its practices and ultimately, its contribution to a more prosperous world.

[9] While the cost savings from information technology applications are important, the lack of widely accepted standardised data transfer protocols among the hundreds of proprietary systems currently being used represents one important hurdle to be overcome before these savings can be realised.

ANNEX I: ISPS CODE PART B: GUIDANCE REGARDING MEASURES TO BE TAKEN BY SHIPS AND PORT FACILITIES OPERATING UNDER SECURITY LEVELS 2 AND 3

Security level 2	Security level 3
Shipboard Access	
• assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access; • limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them; • deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols; establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility; • increasing the frequency and detail of searches of people, personal effects, and vehicles being embarked or loaded onto the ship; • escorting visitors on the ship; • providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance; and • carrying out a full or partial search of the ship.	• limiting access to a single, controlled, access point; • granting access only to those responding to the security incident or threat thereof; • directions of persons on board; • suspension of embarkation or disembarkation; • suspension of cargo handling operations, deliveries etc; • evacuation of the ship; • movement of the ship; and • preparing for a full or partial search of the ship.
Restricted Areas	
• establishing restricted areas adjacent to access points; • continuously monitoring surveillance equipment; and • dedicating additional personnel to guard and patrol restricted areas.	• setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and • searching of restricted areas as part of a search of the ship.
Shipboard Cargo Handling	
• detailed checking of cargo, cargo transport units and cargo spaces; • intensified checks to ensure that only the intended cargo is loaded; • intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships; and • increased frequency and detail in checking of seals or other methods used to prevent tampering by; increasing the frequency and	• suspension of the loading or unloading of cargo; and • • verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

detail of visual and physical examination; increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and/or coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.	
Monitoring Ship Security	
• increasing the frequency and detail of security patrols; • increasing the coverage and intensity of lighting or the use of security and surveillance and equipment; • assigning additional personnel as security lookouts; and • ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided. • Additional lighting may be necessary to protect against a heightened risk of a security incidents. When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.	• switching on of all lighting on, or illuminating the vicinity of, the ship; • switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship; • maximizing the length of time such surveillance equipment can continue to record; • preparation for underwater inspection of the hull of the ship; and • initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.
Ports	
• assigning additional personnel to guard access points and patrol perimeter barriers; • limiting the number of access points to the port facility, and identify those to be closed and the means of adequately securing them; • providing for means of impeding movement through the remaining access points, e.g. security barriers; • increasing the frequency of searches of persons, personal effects, and vehicle; • deny access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and • using of patrol vessels to enhance waterside security;	• suspension of access to all, or part of, the port facility; • granting access only to those responding to the security incident or threat thereof; • suspension of pedestrian or vehicular movement within all, or part, of the port facility; • increased security patrols within the port facility, if appropriate; • suspension of port operations within all, or part, of the port facility; • direction of vessel movements relating to all, or part, of the port facility; and • evacuation of all, or part of, the port facility.
Port Restricted Areas	
• enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion detection devices; • reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses; • restrictions on parking adjacent to berthed ships; • further restricting access to the restricted areas	• setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied; and • preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.

and movements and storage within them; • use of continuously monitored and recording surveillance equipment; • enhancing the number and frequency of patrols including waterside patrols undertaken on the boundaries of the restricted areas and within the areas; • establishing and restricting access to areas adjacent to the restricted areas; and • enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility.	
Port Cargo Handling	
• detailed checking of cargo, cargo transport units and cargo storage areas within the port facility; • intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and then loaded onto the ship; • intensified searches of vehicles; and • increased frequency and detail in checking of seals and other methods used to prevent tampering. • Detailed checking of cargo may be accomplished by some or all of the following means: .1 increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination); increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and coordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.	• restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and • verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.
Monitoring Port Security	
• increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage; • increasing the frequency of foot, vehicle or waterborne patrols, and • assigning additional security personnel to monitor and patrol	• switching on all lighting within, or illuminating the vicinity of, the port facility; • switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and • maximizing the length of time such surveillance equipment can continue to record.