THE POLITICAL ECONOMY OF MARITIME CONTAINER SECURITY

Kenneth Button* and Marc Thibault

Center for Transport Policy, Operations and Logistics
School of Public Policy
George Mason University

ABSTRACT

The September 2001 attacks in the US raised significant concerns that containers may be used to carry out or facilitate terrorist attacks. The very large number of containers, the thousands of firms and the multitude individuals involved in container shipping, and limited government oversight over the global supply chain makes confronting this concern difficult. Further, organized crime has long used containers to smuggle narcotics, weapons, people and other contraband making it reasonable to assume terrorist groups may utilize containers to further their own ends. Containers are, however, an integral component of a global supply chain that has been designed to be fast and efficient. A terrorist attack that utilized containers and the maritime supply chain could not only damage the short and long-term credibility of the entire global logistics system, but it could damage the psyche of a nation's citizens. Terrorism is ultimately about inflicting psychological damage. A loss of faith in the integrity of the world's maritime shipping system would represent a major terrorist victory. The focus of this study is not on the technical apparatus available to enhance container security, but rather on the institutional and economic factors that will ultimately influence the effectiveness of security policies for the maritime shipping network.

INTRODUCTION

International trade has grown over the past decades in part due to international initiatives involving multinational and bilateral relaxation to institutional barriers to international commerce, but also as the result of important managerial and technology developments. The result has been the creation of sophisticated supply chains that has reduced the costs of trade in goods, and opened up a variety of new markets. Recent concerns over the security of this structure are, however, beginning to increase costs in the supply chain both directly as new security measures are legislated, and indirectly as the free flow conditions in the chain are impeded by these measures.

Security has always been an important aspect of the supply chain. In recent years, however, the nature, scale and scope of security concerns have changed. In the past, container security centered on the prevention, or at least containment, of theft and smuggling through security related activities carried out by shipping firms, private security companies, government agencies, and international cooperation between nations.

The interest now extends from these traditional involvements to embrace the concern that terrorists[1] may use the container supply chain either to carry out a large-scale terrorist act or to smuggle the material required for a terrorist attack[2]. The impact of the September 2001 attacks in the US has brought to the fore the potential scale of the damage and loss of life that can accompany a planned attack using the transportation system[3]. While the attacks in New York and

Arlington involved commercial airliners, there is the possibility that the container supply chain could be used, albeit in a significantly different way, to cause similar social impacts.

Containers and unitization have played an integral part in the development of global supply chains since the 1960s. They reduce shipment times and costs (including costs associated with theft and damage) by minimizing the amount of physical handling of goods during transit. Containers, in conjunction with the deregulation of transportation markets, the application of information technology, improvements in fuel efficiency, and opening of markets, contributed to the development of global supply chains, and notably just-in-time production. Containers have also contributed to the consolidation of maritime transportation, and the growth of massive transshipment ports, merging of shipping companies and global alliances, and larger vessels that are handling an increasing share of the world's container traffic.

The focus, here, is on modern terrorist security issues that surround containers as they flow through the global supply chain. There is an estimated 11 million shipping containers in use (World Shipping Council, 2004) and it is anticipated the number will continue to grow (United Nationals Commission on Trade and Development, 2003). Thousands of firms and individuals, who traditionally have not been subject to rigorous regulation and oversight, pack, handle or utilize shipping containers. Containers pass through major urban areas and other vital infrastructures as they are being transported to their destinations. Most governments do not have the resources to guarantee the security of every container within its jurisdiction (Flynn, 2004). Further, just-in-time logistics means that container security related initiatives that slow down international trade push up inventory costs, and ultimately prices.

There is an emerging body of literature pertaining to terminal and transshipment security, albeit often technical in nature. The security of containers has become an important policy issue since September 2001[4]. This is because the transportation of containers is critical activity of the global supply chain. In this sense, the transshipment of containers is seen to meet the criteria of critical infrastructure as defined by the US General Accounting Office (2002a).

> CIP [Critical infrastructure protection] involves activities that enhance the security of our nations' cyber and physical public and private infrastructure essential to national security, economic security and public health and safety … [suggesting] existing challenges; Develop a national CIP strategy; Improve analysis and warning capabilities; Improve information sharing on threats and vulnerabilities; Address pervasive weaknesses in federal information security.

The paper pulls together what is known about the security risks for shipping containers, and the measures that have been implemented to combat these risks. It discusses the importance of the maritime shipping industry in the container supply chain, and exams the policy implications of maritime shipping industry's hub and spoke structure. It looks at both the incentives of the various actors to optimize the security of containers and at the public policy responses that may be necessary where market incentives fail. It discusses major mandatory and voluntary initiatives that have recently been undertaken to enhance the security of containers.

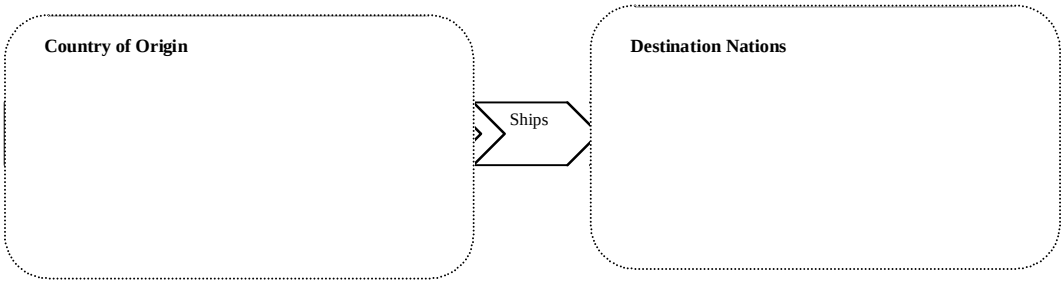
CONTAINER SHIPPING

Initially it is useful to highlight a few of the key features of the maritime container industry, one of which is its network structure. Maritime shipping is a critical link in the global container supply chain. There are three main container trade routes: Asia-US, Asia-Europe, and Europe-US

In 2003 the total value of the manufactured goods on these routes was $938.5 billion (World Trade Organisation, 2004). The Asia-US trade route is largest container route accounting for approximately 41% of TEUs shipped on these trade routes. It is estimated that in 2003 the value of trade in manufactured goods between Asia and North America was some $339.8 billon and accounted for 43% of the value of the major regional flows of manufactured goods. The Asia-Europe is the second largest container trade route. In 2003, the value of trade in manufactured goods between Asia and Europe was $282.3 billon and accounted for 30% of the value in the interregional trade of manufactured goods. The Europe-US is smallest trade route with the value of the manufactured goods traded between these regions in 2003 estimated to be $256.5 billion and accounted for 27% of the value of the major interregional trade flows of manufactured goods.

The majority of the world's non-bulk cargo is transported in maritime shipping containers. The maritime transport of containers, however, is part of a larger complex global supply chain (Figure 1) that involves numerous actors located on different continents. A typical voyage of a maritime shipping container can involve up to 25 actors, generate 30-40 documents, use 2 to 3 modes of transportation, and be physically handled at up to as many of 15 locations.

Non-Bulk cargo enters the container supply chain by being palletized and placed in shipping containers by its manufacturers or an intermediary forwarder. Transportation firms convey the loaded containers to ports where they are cleared by customs and loaded on ships. The containers then are transported to a final destination port where they cleared by customs and transported to its final purchaser or distributor. A container, during its voyage through the global supply chain, may be placed in temporary storage for extended periods of time as it waits for the availability of further transport.



Source: Adapted from Organisation for Economic Cooperation and Development, 2003.

Figure 1. The International Container Supply Chain

The maritime segment of the global container supply chain is a hub-and-spoke system of ports and shipping services. Such systems offer major commercial benefits in the form of economies of scale, scope, and density (Sly 2001). To benefit from scale economies ports and maritime

operators maintain capital-intensive operations and have placed a heavy emphasis on increasing the number of containers they handle. Economies of scope occur when firms can spread their costs by offering a range of services. Ports and maritime operators do this by providing access to world ports, transportation modes, and other container related services. Economies of density occur when the presence of a network hub results in average revenue increases that are greater than the number of services provided. Ports and maritime operators provide this benefit because they provide land locked producers with access to other ports and markets that would otherwise be unavailable.

The operations of the world's ports and maritime operators are interdependent and interact with the rest of the container supply chain. A lack of security at one port, at the maritime operator's facilities, or ships may expose other ports and maritime operators, and other firms in the supply chain to security risks. A terrorist attack on a container port, or on the facilities of a maritime operator, may damage critical infrastructure and result in a costly disruption of the container supply chain. A container based terrorist attack could have the effect of shutting down, or dramatically slowing down, the supply chain. This would occur when government officials and private firms face uncertainty in not knowing how many container based attacks are in progress (Flynn, 2004). Therefore, they would likely take action to ensure the security of the entire container supply chain.

There are over 4000 ports in the world but 20 account for 45% of the world's throughput of container TEUS. Ten Asian ports accounted for 35% of world's TEUS whilst 6 European ports accounted for 11% and 3 North American ports account for 7%. The Middle Eastern port of Dubai accounted for 2%. This geographic distribution of the world's largest 20 containers ports has significant policy implications. The security of the maritime container supply chain is only as strong as it weakest link. A lack of security at one port may expose other ports, maritime operators, and firms in the supply chain. Container ports require extensive capital and facilities to efficiently operate. A terrorist attack that inflicts major damage on a container port could render seriously disrupt the global supply chain if there is not be the existing infrastructure to efficiently re-route containers. This could have a negative effect of many national economies as the global supply chain is an integrated one.

There is also a concern regarding national sovereignty that is associated with container security. Twelve nations have ports that are in the top 20 container ports. This means that any effort to enhance the security of the supply chain will require significant cooperation between at least twelve countries. Each of these countries has national security interests and priorities. Thus, any solution to improve maritime security will require a cooperative effort that seeks a satisfactory solution rather than the optimal security solution. This challenge is further compounded because any effective solution must also include nations who have smaller container ports.

Maritime shipping operators act as spoke in the maritime container supply chain as they transport containers between the world's container ports. The largest 20 container service operators account for over 60% of the world's fleet TEU container capacity in 2002. Asian firms accounted for 11 of the top 20 container service operators and approximately 27% of world TEU capacity. Five European firms appear in the list and constitute about a quarter of the world's TEU capacity. Competition between maritime operators is primarily between shipping networks. Therefore, firms are going to resist any security initiative that they perceive will have a negative impact of the competitiveness of their network relative to the competitiveness of other maritime networks. This resistance to regulation is further compounded by the fact that there are maritime operators not on the list that are capable of rapidly gaining market share.

CONTAINERS AND TERRORISM

Containers as Weapons

Containers offer a potential threat to security not only because of their number and mobility but also because of the role that they play in the global economy. Producers use containers in increasingly integrated systems to transport material and goods by all mechanized modes of transportation. They inevitably pass through vulnerable areas where an attack may not only cause economic damage but also result in deaths and injuries to the population. A terrorist attack that utilizes shipping containers can, therefore, not only have cause damage at the location of any incident but can also potentially have significant consequences on the global supply chain in terms of pushing up the costs of distribution. A container based terrorist attack can affect the container supply chain in four broad ways[5]:

- Supply Chain. A terrorist attack that utilizes a shipping container could in the short run have the effect of dramatically slowing down the global supply chain. Besides any immediate collateral damage, government officials and private firms would be forced to check the integrity of the containers to verify that containers would not be used to launch additional terrorist attacks (Flynn 2004). In the long run, nations and firms that do not provide acceptable levels of security would see a decline in the number of containers they handle. This would have a corresponding effect on their economic wellbeing.

- Terminal shock. Size is important for the economic vitality of ports and other logistic centers that handle containers. These distribution centers compete to be the largest and to have the greatest number of container related services. Potential customers like the economies of scope that accompanies this; they have a wide diversity of outlets from which to select container related services. The larger the container distribution center, however, the greater the potential it has to become a terrorist target. This may lead to trade-offs in term of size of container distribution centers and the degree of confidence that customers have in them.

- Scope and Density Economies. Container distribution centers offer significant benefits to their customers and firms. If large container distribution centers because of the fear of being targets for terrorism are seen as untenable, then this will lead to a dispersion of container related activities and the loss of the scope and density economies that accompany hub-and-spoke networks.

- Geographical. Container distribution centers are not inexpensive to construct. They also have significant concentrations of capital machinery. Any terrorist attack that inflicts serious damage to a container distribution center will result in significant costs being added to the value chain. These costs will not be in global terms but they will have implications for the relative attractiveness of different centers and thus will have impacts on the spatial distribution of containers.

Taken in this context, security is a multifaceted challenge and all of these facets are relevant to the maritime shipping. There become a number of generic stages involved in the handling of these terrorist related security issues. These apply with particular nuances to the security of maritime shipping containers.

Prevention

The prevention of an act of terrorism is a clear initial line of defense.[6] The container supply chain is a global network in which one actor's outputs serve as inputs to downstream firms. Individual firms, however, can only do so much to prevent terrorists from violating the integrity of a shipping container.

Much of the enhanced security at ports and at sea has to do with the international sharing of intelligence. Ports and maritime shipping companies are inevitably becoming involved in this through the exchange of information and involvement with local, national, and international security agencies in terms of being vigilant to known dangers. Internally, because making change in basic architecture is generally difficult and expensive, ports and maritime shipping companies can enhance their overall security by improving their physical security. They can restrict access to containers by initiating personal identification systems, developing security zones, hiring more security personnel and installing more security related equipment (lights, fences, surveillance cameras, etc).

Containment

The vulnerability of the entire container supply chain makes it economically inefficient to put in significant measures to provide a total guarantee that an individual container will not be used for a terrorist acts. This is often, not a simply a matter of financial considerations, although these are not unlikely to be unimportant, but can reflect significant economic costs that may accompany effective prevention options. An increase in the number of security measures increases the likelihood that a container may be stopped in transit for a variety of reasons. These measures, if there are too many or are especially burdensome, can negate the economic benefits of containerization.

Ports are normally designed to facilitate quick access to other transportation modes. As a secondary measure, therefore, there may be design and operation measures that could be implemented to reduce or localize the impacts of a container being used for a terrorist attack. All of these types of measures, however, can make it more difficult for containers to move through the port. But beyond this, more specific measures may involve locating potentially dangerous material such as gas tanks away from widely used areas, dispersing critical equipment and facilities, and building additional transportation structure so that a terrorist attack on a port would not affect the entire complex or the entire supply chain. These actions, however, may require significant investments in additional infrastructure.

Treatment

The primary element of treatment in the US and other countries is that of rapid and appropriate response. Essentially, this is a reactive rather than a proactive approach to any terrorist attacks. Many ports and maritime shipping firms have altered their operational procedures and enhanced their security measures since September 2001. Formerly, these were designed to deal with natural emergencies or accidents or to reduce the theft rather than purposely driven efforts to use the maritime transportation system for terrorist purposes. Many maritime firms and ports are now working closely with local, national, and international organizations to design structured measures should any attack terrorist act take place. However, governments and international organizations may have to get involved in planning a response to a terrorist attack on a port as the attack may seriously disrupt national and international supply chain.

In practice, a strategy based upon a response approach to any terrorist attack has the advantage that it is does not completely shut down a port's operations or the maritime transport of containers. Given the importance of maritime shipping and the potential costs involved this latter

consideration is not trivial. It can also be fitted into wider response strategies for a region or for the longer supply chain. This response can also be based upon a large base of diverse experiences drawn not necessarily from terrorist incidents but also from other major incidents such as earthquakes or engineering failures (Jackson et al, 2002).

ECONOMICS OF MARITIME SHIPPING AND CONTAINER SECURITY

Much of the reaction to the 2001 attacks on the US mainland was essentially a knee-jerk reaction. Politicians felt that something should be done to maintain public confidence and action was the natural recourse. There are, however, opportunity costs inherent in any actions, and gradually this has been explicitly recognized. The economic implications of revised security measures, for shipping and other sectors, are still imperfectly understood from an intellectual standpoint and quantification of the key economic parameters remains primitive if attempted at all[7].

Strictly, just as there is no such thing as shipping economics, so there is no such thing as the economics of maritime shipping and container security. What exists is a particular market that has associated with it a number of imperfections that can result in a socially sub-optimal output. In the case of maritime security a number of, in some cases inter-related, market features would seem pertinent.

Measurement of the Costs of Security

Security is not costless. Its measurement, however, is not simple. In terms of any individual security measure there are usually fairly well defined direct financial costs, although these often only become explicit *ex post*. Secondary costs, external to the immediate costs of the measure, can be large and often difficult to quantify. The most clear cut case are the additional costs of inventory holding, handling, and transportation associated with searches of containers or the production of extra documentation. Direct costs are bourn by the authorities, and the indirect costs by shippers and ultimately users of the supply chain. These are, however, essentially accountancy issues that can be dealt with in a full cost framework, although in practice this is seldom done. More difficult to evaluate are the costs to the macro economy of additional security measures.

National income accounts are essentially based on a framework developed by John Hicks in the 1930s and operationalized, albeit in slightly different ways, by Richard Stone and Simon Kuznets in the 1940s and 1950s. They are rooted in Keynesian economics are designed to provide measures of income that correlated with employment levels. Consequently, it is quite possible for an increase in security activities, including those involving maritime activities, in response to a terrorist threat to result in a higher national income than a situation where no such threat exists. The way that national income is calculated was never designed to cover security situations and is a very imprecise, when not perverse indicator of the national costs of major security initiatives.

There is another side to the issue, and one increasingly being highlighted by the public choice school of economics, involves the social costs of enhanced security, and in particular its costs in terms of individual liberties. State interventions in markets inevitably remove personal property rights and limit individual freedoms. Container searches and more detailed inventories are seen as part of this erosion process. These are not factors embedded in national income accounts, but are additional costs to society.

Risk and Uncertainty

There are also challenges on the demand side for anti-terrorist measures. A particular problem is that there are issues of both risk and uncertainty to be considered when examining the policy

issue of container security. Risk has a statistical probability associated with it while uncertainty does not. This means that under most circumstances it should be possible to insure against risk but not uncertainty. Whether an individual chooses to insure, or to take the risk burden himself is sometimes a quasi-subjective matter revolving around whether it is felt the premium for the insurance is worth the security offered. It is a question of how information is subjectively treated rather than a case of a lack of information. In other cases, if the implications of the outcome affect third parties there are often institutional requirements to have insurance, as many countries insist automobile drivers do.

With uncertainty it is more a matter of the judgment of those affected. In the absence of a Gaussian probability, then Bayesian views come into play. Holding an arbitrary 'reserve' to cover losses is one approach, but not normally practical for major events. This is often why government acts to provide compensation after an adverse and unpredictable event such as an earthquake – 'An act of God'. Terrorist attacks are infrequent, and diverse in their nature and in their impact making risk assessment virtually impossible. This is why in many cases the government provides at least a minimum level of cover.

One of the difficulties with providing the optimal level of security for shipping containers is the actions of those involved are motivated by Bayesian ideas of risks, subjective probabilities rather then by Gaussian risk, objective probabilities. This means that from a statistical perspective a terrorist event using containers can cause an over-reaction from governments, maritime shipping firms, and the general public. There may also be an excessive perception of the risks to shipping containers in the maritime shipping network. Further, there may be unwillingness by the general public to accept an objective level of risk even if its provision is based upon hard data.

An additional difficulty in the provision of container security is asymmetric information where one party has significantly more information than other market participants. Governments, in order to effectively provide for their national security, cannot provide the public with a complete intelligence assessment of the risks facing the nation's container supply chain. Equally, shipping companies have no commercial incentive to highlight the potential terrorist hazards that containers may pose. The general public, generally speaking, is rationally ignorant of the potential dangers facing their nation faces and thus its desire for container security will be driven more by perceptions rather than by facts. The public, however, is not unaware of the general threats that are posed and in these circumstances tend to be highly risk averse fearing that the authorities are hiding more than they are revealing (Ackerlof 1970). They will thus seek higher levels of security than would prevail in conditions of full information.

Full information on the risks to shipping containers and a Gaussian approach to the treatment of risk, makes it relatively simple to determine the amount of resources to devote toward container security (Figure 2). It is conceptually possible, with both the costs and benefits rising with the increased provision of security, using a simple cost-benefit calculation to determine the optimal security level of S_1. If, however, the risk is unknown there is a tendency for the cautionary principle to be applied and for the benefits of security measures to be over valued. If there is asymmetrical information, or at least the perception of asymmetric information, between the government and the general public then the precautionary effect is likely to be larger. This can then lead to excessive security at a level S_2. More importantly, there is, from a conceptual perspective, even the possibility that that the benefit and cost curve are not seen as intersecting because subjective risk assessment results in the perceived benefits of enhanced security rising faster than the costs of implementing additional security measures. As a result, there is perceived to be an infinite net benefit for increasing container security.

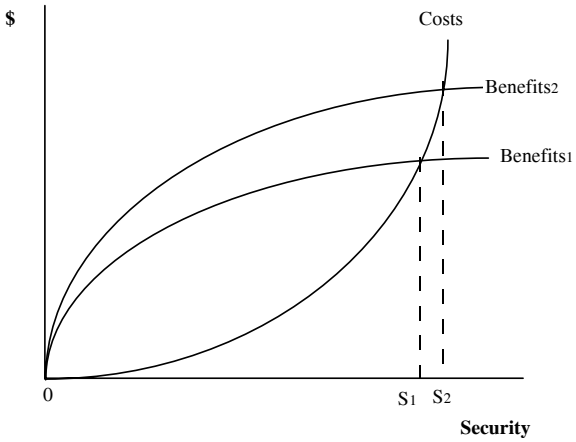


Figure 2. Optimal Security Expenditure

To retain public confidence in shipping as part of global logistics structure there is a need to ensure that the dangers of terrorist attack are kept within acceptable social limits. There are clear issues about the best ways of achieving this in a purely technical sense, e.g., what should be the role of technology and what form should it take? But there are also more basic issues of the roles of the various interested parties in achieving optimal levels of security.

In general terms the actors can be broken down into those with a private incentive to ensure appropriate security within maritime activities and those that have a more indirect social motive in wanting to serve the 'public interest'. The security goals of these two groups diverge. The first group, driven by Adam Smith's invisible hand, will react to the profit motive and ensure investment in security that is consistent with it maximizing its net income but not consider external effects. The second group will be more inclined to see numerous market failures that allow security issues to slip through the invisible hand and lead to a socially inadequate level of security. They will favor public policy measures and possibly public expenditure, to combat these failures. That is, they will favor policies that provide a higher amount of security related efforts than provided by the market. In practice, there is a *de facto* deployment of both the commercial and public interest views of security in the ways in which strategies are developed. The balance is often determined implicitly by a weighing up of several factors (O'Hanlon, et al, 2002).

The extent to which the public and private sector act rationally in response to risks does not always appear to be related to information before them. For example, the public perceives that airline travel is often seen as more dangerous than driving a car whereas very well known statistics show the opposite.

Private Incentives of Logistics Firms

Traditional economic theory assumes that private sector interests will in the presence of markets result in actions to contain such things as terrorism, and indeed it is clear that the insecurity of containers in the maritime shipping network potentially has both a commercial and a social cost.[8] Commercial risk of physical damager can be insured against at a cost, but losses associated with a loss of business are normally uninsurable, or are at least there are ceiling attached.

Firms in the maritime shipping network have a commercial interest in providing an acceptable, if not optimal level for the containers that they handle. Maritime shipping firms and their customers are naturally concerned with the safety and security of their goods in transit. Further, they both

have spent considerable effort to build up their own unique customer franchises and quality of service and need to protect their investments.

The demand for container-based services is a derived demand; derived from the producers and distributors of products. Individual firms will simply adopt the Tiebout (1956) approach if there are unacceptable levels of container insecurity – they will vote with their feet and take their shipping needs to maritime shipping outlets that offer acceptable levels of security. Maritime shipping firms would have to retain their clients by offering more services and less profitable shipping rates. The problem is compounded because insecurity not only reduces affects individuals business but it can affect ports and nations.

Maritime shipping firms may be cognizant of these types of effects and may act to minimize risk, but objective assessment of many elements may be blurred. But the insurance market can often interject a clear, actuarial view to the decision process. Basically, if a maritime shipping firm has insecurities in its operations then this would be reflected in their insurance costs. The problem is that insurance is based upon previous experiences and these may be too limited to provide a reasonable estimate of the magnitude of the actuarial risk involved. Insurance companies will then itself exercises judgment that inevitably tends towards risk aversion. Premiums would be sub-optimally high.

The Public Good Issue

There are numerous individual firms that handle containers as they flow through the maritime shipping network. Each individual firm operation is interdependent with the operations of other firms. Thus, any major terrorist event will almost inevitably have severe repercussions for firms throughout the maritime shipping network. As a result, there is very little incentive for any individual firm to enhance its security arrangements- if other firms in the maritime shipping network have lower levels of security then there is no significant advantage in increasing its own.

On the other hand, each firm in the maritime shipping network benefits if other firms increase their security and they cannot be excluded from enjoying those benefits. In this sense, security can be seen as meet the economists definition of a pure public good in that it has significant elements of both non-excludability (one cannot be excluded from the benefits enjoyed by the actions of another) and non-rivalness (one's consumption of a good provided by another does not diminish the latter's consumption)[9].

In market conditions, because a lack of a financial incentive public goods are underprovided and require some form of external public policy to either coerce the appropriate supply from the private sector, or for the state to provide the public good itself; national defense is often cited as the classic case of a public good.

An optimal container security policy involving the public sector bearing the uncertainty and the private sector, through insurance markets, any risk would mean some private actions by those directly with involved the shipment of containers with national and international authorities having a more public role. In this sense, there is essentially a need to rethink container security in terms of an interdependent network rather than the security of individual containers. Both public and private interests come into play, but teasing out the exact role of each and their implicit financial contributions, is difficult.

Capture of Security Policy

There is economic rent to be derived from the supplying security services. There are profits to be made by offering consultancy advice, providing hardware, policing security systems, etc.

Inevitably there is a tendency for various groups to capture these rents. Given the involvement of political considerations there is also the prospect of capture by those responsible for defining the framework of the system (essentially 'pork barrel politics) and by those who oversee it (Stigler, 1971, Posner, 1975). Given the costs of securing the maritime sector, the need to coordinate special skills that may be needed, combined with the nature of the uncertainty involved, some form of government involvement is inevitable. While some of the security measures may be undertaken directly by government agencies, there has been a trend towards outsourcing in many areas, but most notably utilities, over the past twenty years. The intent is to ensure that X-inefficiency is minimized and thus the maximum level of security can be attained from a given budget. Tendering has become commonplace as potential suppliers compete for the market (Demsetz, 1968).

The problem with this in the security context, beside a plethora of challenges with defining an appropriate auctioning system, is that of quality control. Tendering can be done in a number of ways. In many cases a clear output is specified and the supplier will to provide this at lowest cost wins the contract. This sort of approach has been used in such domains as airport screening of passengers, and has potential for the screening of maritime containers. Security patrols at ports offer another possibility. The difficulties lie in two broad areas. There is the need to define an appropriate level of security service to be tendered for. This often requires rather precise descriptions that may prove inappropriate, or criteria that meet political expedience rather than strict security logic[10]. Added to this, contracts are usually for a defined period that gives little flexibility to react to changing circumstances during the contract. Second, there is scope for capture of the system by the private companies offering services. This can be at the initiation level of tendering as these companies lobby the political process for criteria close to their own 'product'. It can also be at the renewal phase if there are fixed costs or economies of experience that give incumbents an advantage.

International Externalities

Maritime transportation has a large international component to it. Security is only as good as the weakest link in the system and this may be threatened by a lack of international incentive to prevent attacks on the logistics chain. The problem may be seen in this context as a failure of governments to agree on a mechanism for property right allocations because of the capture of the system by their own populations. An example of this is that many states have failed to implement security agreements in the past[11]. The underlying challenge is that there are failures in the institutional structure to handle such international issues; a problem that can be illustrated using Figure 3.

The figure depicts the marginal domestic benefits (MBD) associated with a single country imposing maritime security measures. Conventional notions of diminishing returns suggest that the benefits of increasing levels of security diminish as additional measures are added. For simplicity it is assumed that there are no critical levels. The benefit function ignores the benefits to other nations of this single state acting to enhance its own security levels. If these benefits to other countries are added in, the resultant international marginal benefit (MBI) curve lies further out. The tendency is for domestic governments, however, to effectively become free riders in these circumstances. They may advocate global interventions to prevent terrorism, but do not have not any incentive to take their full share of responsibility for doing so. If the MC curve in the diagram is the marginal cost of security for the individual country, then without appropriate international cooperation the incentive for the single country is to only move to point A_D rather than the global optimum of A_I.

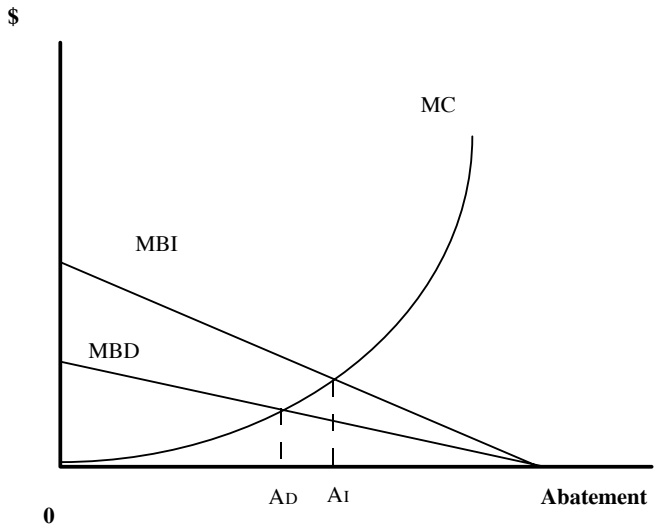


Figure 3. Government failures to internalize maritime security threats

The problem here may be seen as one involving an inherent market failure but in fact it is combined with an institutional structural failure that prevents effective governmental actions to overcome this. This type of situation generally arises in situations where there is no internationally agreed ownership of property rights such as over the oceans, and it has been a long-standing issue concerning such things as piracy.

PUBLIC POLICY RESPONSES

The events of September 2001 have brought forth major institutional changes in the US. That have amongst other things, culminated in the creation of the Department of Home Land Security and with changes in the way the military looks at homeland security (Larson and Peters, 2001). There have been major legislative measures aimed at coordinating the activities of the various security agencies. There have also been very many more localized state and metropolitan initiatives to tighten security. In addition, a concerted effort has been made to involve the private sector in the formulation and implementation of new security initiatives. The optimal division of responsibilities between the various levels of government and the private sector is not, however, an uncontentious issue.

In practice, the issue of the degree of public policy involvement in ensuring optimal security of the container supply chain is essentially one of political economy, the pure theory of public goods and externalities is well developed but judgment is required in its application. Of more practical importance are the natures of the policy tools that could be deployed. There are several approaches in these circumstances that can be pursued to the adopting of public policy measures to protect private property (Litan and Orszag, 2002). None are without their problems.

In very broad terms these can be divided into the following groupings.

Regulations

The imposition of command-and-control regulations is often the natural reaction of policy makers to issues such as security. They favored because they are usually simple to understand, impose, and monitor. They have the fiscal advantage for the authorities that their costs are largely borne, initially at least, by the private sector; in the context of shipping containers, regulations could

include such things as the specifying of specific types of technologies used to prevent container tampering, locating devices, and more detailed documentation. The passing of costs to the industry is often not simply a matter of financial expediency on the part of the authorities, but can also reflect ease of passing necessary legislation without having to engage in complex and time-consuming budgetary processes.

Economists, however, regularly point to the generic inefficiency of command-and-control measures as opposed to other instruments (Baumol and Oates, 1988). Because they seldom equate marginal costs across those that are affected by them they are usually an unnecessarily expensive way of attaining a given level of security. In addition, on their own they offer only a minimal incentive for the given level of security to be exceeded. In the case of shipping containers, there is the added problem that regulations may tend to be to rigid in their application which may be undesirable in the context of terrorism where there is little previous experience upon which to base regulations.

Insurance Requirements

A particular form of command-and-control policy is to pass the property rights for safety to the private sector. This involves either specialized insurance markets or self-insurance playing a large role. The statutory need to have insurance is common for such things as banking, practicing medicine and automobile driving. In the context of terrorism insurance in shipping it provides a stimulus for introducing security measures and provides a safety net should security measures fail.

The problem is that in very many cases of terrorist threats, insurers will not provide cover – actuaries work on risk-based estimates of an event occurring and its magnitude, but with the potential threat of maritime container based attacks there is insufficient data to estimate this risk and premiums, and hence incomplete insurance markets exist. Wherever, cover is offered, the natural tendency for the insuring company is to levy high premiums to ensure their own financial position is more than off-loaded. More fundamentally, there may emerge the underling problem of any insurance market, namely that of a moral hazard. Some firms in the container supply chain may take taking out minimum levels of insurance rather than improving their security system to the average level anticipated for the premiums being paid.

Subsidies

Where security involves a genuine public policy element there may be a case for public subsidies to cover the costs of security. This has traditionally been the reason for having the state provide defense and police services. Since the measures are being deployed for non-commercial reasons and where profit-maximizing criteria will not produce the perceived socially optimal level of security. Subsidies may also be supported in cases where legal constraints prevent an insurance market from functioning effectively, e.g. where the legal limits on the exposure of insurance companies losses. Subsidies may either be in the form of direct assistance (e.g. part of the costs of maintaining container security) or as an insurer of last resort (e.g. offering reinsurance) should the private sector market prove inadequate. Issues inevitable arise with any form of subsidy as to the point at which private sector matters require public finances.

There are a number of problems with using subsidies that can affect the behavior of private, commercially motivated undertakings such as shipping firms and ports.

- They can lead to the use of unnecessary security elements (‘gold-plating of the security system’). If the state is paying there is no reason to be frugal.

- The system can be captured by vested interests, often those with powerful lobbying voices that can lead to excess security or inappropriate security measures.
- They can provide resources for security upgrading for undertakings that would have been taken in response to commercial pressures anyway. This can be seen as a sort of crowding-out argument.
- Subsidies are paid for from general revenues and inevitable questions of fairness as well as efficiency arise.
- Given the network nature of maritime container activities, there is the possibility of free-riding by those in other parts of the supply chain. This may also extend across national borders; if one country enhances its security it may reduce the incentive for others to do the same.

CONTAINER SUPPLY CHAIN SECURITY INITIATIVES

Given these economic challenges and the instruments available to tackle them, the question arises as to how the authorities are handling them? It is now feared that the terrorists may use shipping containers to carry out large-scale attacks against civilian populations (Flynn, 2004). The security of the container supply chain, however, was not a major policy concern in the US until the September 2001 attacks. Prior to this, governments and firms focused their efforts primarily on minimizing container theft and container based smuggling. The recent actions, however, appear more as ad hoc initiatives rather than a carefully worked through and appraised strategy. Much of the specific activities have been at the international level involving some degree of public/private partnership with incentives for the private sectors to participate. They have also sought to engage those at the other end of the international supply chain. Added to this explicit maritime activity, there have been linked initiatives involving land surface transportation at the interface with the maritime leg of a freight movement.

By definition almost, full details of what is being done to combat the threat of terrorist use of containers is lacking. Some of the more transparent actions, however, do in principle if perhaps not in their detail seem to be meeting a number of the economic issues that seem relevant.

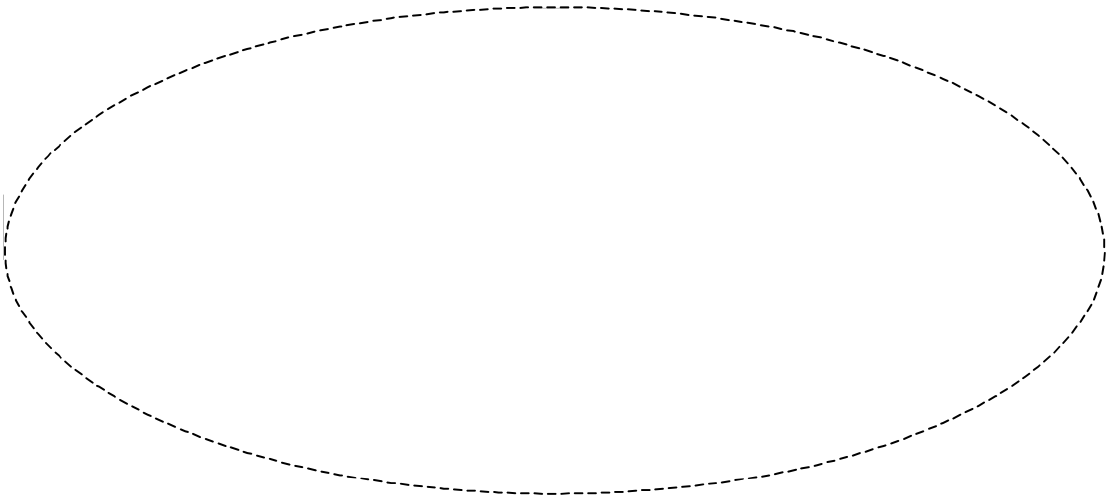
Dealing with International Externalities

The International Maritime Organization (IMO) and the US have since sought recourse to command-and-control measures and have implemented several mandatory and voluntary policy initiatives to improve the overall security of the global container supply chain (Figure 4). The mandatory initiatives are designed to improve the security of the maritime segment of the container supply chain while the voluntary US led initiative is designed to improve the general security of the entire container supply chain.

The IMO, in response to the September 2001 attacks and the increased concerns about maritime security, adopted the International Ship and Port Facility Code (ISPS) in December 2002 (International Maritime Organisation, 2002a; 2002b). The ISPS sets forth mandatory security requirements that must be taken by governments, ports, and shipping companies to enhance the security of the world's maritime transportation system. These mandatory requirements went into effect on 1 July, 2004.

The ISPSC is structured risk management effort. Individual governments are required to assess the risks facing their ports and establish a three tiered security system in which 1 is associated with normal level of security threats, 2 with medium level of security threats, and 3 with a high level of security threats. The code requires that as a minimum, ports, maritime operations, and

ship establish security plans that correspond with the three security levels. These security plans should indicate the operational and physical measures required to comply with the three security levels. They must also designate security officers that are responsible for ensuring that their facility or their organizations facilities comply with the requirements associated with each maritime security level. Finally, they may have obtain and operate the specific types of equipment as specified by the ISPS Code.



Source: Adapted from Organisation for Economic Cooperation and Development (2003)

Figure 4. International Initiatives to Secure the Container Supply Chain

The US Maritime Security Act of 2002 is the country's legislation for meeting the requirements set forth in the ISPS code. The MST, however, has two requirements that exceed the minimum requirements of the ISPS Code. First, it requires the establishment of Transportation Security Cards for port personnel and new seafarer identification paper if negotiations at the International Labor Organization fail to yield these two initiatives. Second, it requires that the US government not only assess the security plans of foreign ports but it must also assess the effectiveness of a foreign nation's security oversight.

The intents of ISPS Code and its US enactment are to establish a risk-based approach to maritime security that will promote the free flow of trade while at the same time provide an international security framework. The problem is that the underlying problem is not one of risk but that of security and thus the various designations of security threat are essentially educated guesses rather than probability based criteria.

Network Considerations

The Container Security Initiative (CSI) is a US led effort based on the premise that the US's borders the country's last line of defense (US Customs and Border Protection, 2004a). Therefore, to reduce to risk of a container based terrorist event, containers should be inspected at foreign ports prior to being shipped to the US. The US has implemented the CSI by entering into bilateral agreement that allows both nations to send inspectors to each other ports. These inspectors have

the authority to inspect containers that are being shipped by sea to their respective countries. The purpose of the CSI is to enhance the security of the maritime container supply chain between the US and its CSI partners by: using intelligence and information technology to identify containers that may pose a terrorism risk, pre-screening containers that pose a terrorism risk prior to their departure from port, utilizing detection technology that rapidly screens at-risk containers and utilizing tamper-evident containers. There are currently 20 countries that have committed to participating in the CSI and there are currently 32 ports taking part in the CSI.

There are several anticipated benefits of participation in the CSI. It serves as deterrent for terrorist using a CSI port for container based terrorist activities. Containers from CSI ports will spend more time in actual transit and less time awaiting customs clearance. Finally, a CSI port, and it customers, will be able to more quickly resume its operations in the event of a container based terrorist attack.

Private Sector Initiatives

It is recognized that the government does not have adequate resources to inspect all maritime containers entering the US, indeed only about 2% to 4% are currently X-ray inspected at ports. The tax-payer is unlikely, however, to accept the fiscal burden of full responsibility of more checks. The Custom-Trade Partnership Against Terrorism (C-TPAT) is a US program that seeks to develop cooperative relationships between firms in the global supply chain and the US authorities (US Customs and Border Protection, 2004b). Firms that elect to participate in the program conduct a comprehensive self-assessment of their security practices using guidelines developed through the cooperation of the US Customs and private industry. C-TPAT participants must also submit a supply chain security profile to US Customs and also must develop a security enhancement plan that incorporates C-TPAT guidelines. Finally, C-TPAT participants must work toward building guideline into their relations with other firms in the global supply chain.

There are several anticipated benefits associated with participation in C-TPAT. Firms that participate in C-TPAT will be subject to fewer and faster border inspections giving them a competitive advantage to non-participants. They will be assigned an account manager by the US government and will be eligible for account-based processes. Further, the US government will provide C-TPAT firms with a list of other firms that are participating in the C-TPAT program. But the very process of having to conform to C-TPAT requirements has also forced some companies to reassesses their own logistics structures with the result that the net result has an exercise in net cost savings rather than a minimization of additional costs.[12] For this reason the initial scheme proved popular but suggested amendments with a large public sector say in the ways companies approach their internal security raised problems.

Estimated Costs of Container Security Initiatives

To date there has been no full net costing of the initiatives outlined above, nor of the other changes, both with the public and private sectors, that have been initiated to combat the use of maritime containers in terrorist acts. The Organisation of Economic Cooperation and Development's (2003) does provide a few guidelines as to the possible level of the direct costs of the types of security measures now going into place; the OECD is less clear, however, about the potential indirect costs.[13] The estimated initial burden for ship operators of complying with the ISPS Code is of the order of $1,279 million and $730 million per annum thereafter. The OECD is reticent on the costs of the recent US partnership measures because they are less technology driven and open to some flexibility on the way operators implement them.[14]

This general lack of cost assessment, particularly since it is far from clear exactly how effective some of the anti-terrorist measures are, makes empirical analysis near impossible. There also

seems to be little analytical work on the subject despite the considerable burden that the new security measures may have or the social and economic costs that a major terrorist attack would potentially create. In part this lack of cost assessment be as much a reflection of the lack of clarity in the ways the costs of maritime security are to be shared between the various actors involved as in narrow technical accountancy issues.

CONCLUSIONS

Recent years have seen increase in the concern about the security of the container supply chain. The September 2001 attacks have led to new thinking ways containers should be handled. Several of the subsequent security initiatives have involved imposing a direct burden on elements in the supply chain; restricted access to containers, improved physical security, more cargo pre-screening. The immediate burden of these measures has largely fallen on the supply chain and most of the ultimate burden, given the relatively competitive nature of the global market in containers, on final customers. Public moneys have been devoted more to information gathering, coordination, and more traditional policing functions (such as inspections and monitoring).

The difficult from a political economy perspective is that information is scant which not makes assessment of the respective roles of the public and private sector difficult. The problem is compounded by the uncertain nature of the threat that makes it difficult to make rationale choices about the amount of national resources that should optimally be devoted to security in general let alone maritime container security. Traditional cost-benefit analysis is inappropriate for the magnitude of the elements involved and, in any case, is of limited use where there are major issues of uncertainty involved. The ultimate challenge that has emerged involves not only devising methodologies suitable for evaluating large scale initiatives of the type required to cover maritime container security, but also one of ensuring the data at hand offers useful input to the operationalization of the methodology. Judging by the economic literature that has emerged on the subject to date, the exercise is still a work in progress.

ACKNOWLEDGEMENT

This work was funded under a US Department of Justice grant to the Critical Infrastructure Protection Project at George Mason University.

ENDNOTES

[*] Contact author, email: kbutton@gmu.edu

[1] Terrorism is defined as “the systematic employment of violence and intimidation to coerce a government or country into acceding tp specific political demands (New Shorter Oxford English Dictionary, 1993).

[2] Terrorism may entail many micro attacks across various activities aimed at creating widespread panic, or macro attacks on specific structures or institutions aimed at damaging the credibility of those structures. The IRA’s placing letter bombs in mail boxes in the UK would fall under the former heading, their focused attacks on mainline passenger railway stations the latter.

[3] Prior to September 11, 2001, there was a concern that containers would be used to carry out terrorist activities (Flynn, 2000; US Marine Transportation System Task Force, 1999).

[4] The majority of the limited economic literature on terrorism and transportation terminals that exists tends to focus on aviation (Seidenstat, 2004; Coughlin, etc, 2002; Frederickson and Laporte, 2002), railways (Plant, 2004), and seaports (Price, 2004; Organisation for Economic Cooperation and Development, 2003). There has been not yet been extensive empirical economic research on the impact that container security initiatives may have on the container supply chain.

[5] These ideas reflect those expressed by Glaeser and Shapiro (2002) regarding urban form and terrorism into a shopping mall context

[6] Economics is gradually playing a role at the prevention stage of terrorism but contributing to a better understanding of the conditions that create motivation for terrorist acts, including looking at the economic role of religion (Iannaccone, 2004). There is also a literature looking at the way various deterrents affect crime rates (e.g., Becker, 1968) that but this has yet to be systematically applied to matters of terrorism.

[7] For a parallel discussion of these types of issue in the context of air transportation security see Coughlin et al, (2002),

[8] Historically there are numerous cases of private companies acting to secure their commercial interests against terrorist acts – the army maintained by the East India Company in the eighteenth century being perhaps the most formalized.

[9] Finding pure public goods is a difficult task as pointed out by Coase (1974)

[10] The allowing of 4 inch blades on aircraft prior to September 11 being an example.

[11] For example in the context of international air transportation few countries before 2001 fully implemented Annex 17 of the International Civil Aviation Organisation code that governs security matters.

[12] The evidence being reported in the professional media is that membership of the C–TPAT scheme has been beneficial in a number of cases, e.g., results of a survey by Pinkerton Consulting and Investigations Inc. reported in Teach, 2003). A rather obvious observation about the ability of those in the logistics supply chain to find major cost saving with the stimulus of the C-TPAT, is that there must initially have been managerial slack in the system.

[13] The calculations also seem to be in the context of a partial equilibrium analysis with no allowance for any income effects.

[14] The OECD does point out that some costs will be off-set because of technical changes, particularly involving data handling, that were already on-line to be introduced.

REFERENCES

Ackerlof, G.A. (1970) The market for "lemons": quality uncertainty and the market mechanism, *The Quarterly Journal of Economics*, 3: 488-500.

Baumol, W.J. and W.E. Oates (1988) *The Theory of Environmental Policy*, Cambridge: Cambridge University Press.

Becker, G.S (1968) Crime and punishment: an economic approach, *Journal of Political Economy* 76, 169-217.

Coase, R.H. (1974) The lighthouse in economics, *Journal of Law and Economics*, 2, 357-376.

Coughlin, C.C., J.P. Cohen and S.R. Khan (2002) Aviation security and terrorism: a review of the economic issues, *Federal Reserve Bank of St. Louis Review*, September/October, 9-24.

Demstz, H. (1968) Why regulate utilities? *Journal of Law and Economics*, 3: 1-44.

Flynn, S.E. (2000) Beyond border control, *Foreign Affairs*, 79, 57-63.

Flynn, S.E. (2004) *America the Vulnerable How our Government is Failing to Protect us from Terrorism*. New York, Harper Collin Publishers in cooperation with the Council on Foreign Relations

Glaeser, E.L. and Shapiro, J.M. (2002) Cities and warfare; the impact of terrorism on urban form, *Journal of Urban Economics*, 51, 205-224.

Helferich, O.K. and R.L. Cook (2002) *Securing the Supply Chain*, Oak Brook: Council of Logistics Management.

Iannaccone, L.R. (2004) The market for martys, paper to the 116th Annual Meeting of the American Economics association, San Diego.

Jackson, B.A., D.J. Peterson, J.T. Bartis, T. LaTourrette, I. Brahmakulam, A. Houser, and J. Sollinger (2002) *Emergency Responders: Lessons Learned from Terrorist Attacks*, Arlington: RAND Science and Technology Policy Institute.

Knight, F.H. (1921) *Risk, Uncertainty and Profit*, New York: Houghton Mifflin.

International Maritime Organization (2002a) IMO adopts comprehensive security measures, London, IMO http://www.imo.org/home.asp Last Accessed 10 December 2004

International Maritime Organization (2002b) *The Safety of Life at Sea, 1974, As Amended Mandatory Requirements Regarding the Provisions of Chapter XI-2 of the International Convention For the Safety of Life At Sea, 1974, As Amended*, London. IMO.

Larson, E.V. and J.E. Peters (2001) *Preparing the US Army for Homeland Security: Concepts, Issues and Options*, Santa Monica: RAND Corporation.

Litan, R. and P. Orszag (2002) A complicated intersection: public action to protect private property, *Brookings Review*, 20: 20-24.

O'Hanlon, M.E., P.R. Orszag, I.H. Daalder, I.M. Destler, D. Gunter, R.E. Litan, and J.B. Steinberg (2002) *Protecting the American Homeland: A Preliminary Analysis*, Washington: Brookings Institution.

Organisation for Economic Cooperation and Development (2003) *Security in Maritime Transport: Risk Factors and Economic Impact*, Paris: OCED.

Plant, J.F. (2004) Terrorism and the railroads: redefining security in the wake of 9/11, *Review of Policy Research*, 21, 293-305.

Posner, R.A. (1975) The social costs of monopoly and regulation, *Journal of Political Economy*, 83: 807-27

Price, W. (2004) Reducing the risk of terror events at seaports, *Review of Policy Research*, 21, 329-349.

Seidenstat, P. (2004) Terrorism, airport security, and the private sector, *Review of Policy Research*, 21, 275-291.

Sly, O. (2001) *The Economics of Network Industries*, Cambridge, Cambridge University Press.

Stigler, G.J. (1971) The theory of economic regulation, *Bell Journal of Economics and Management Science*, 2: 3-19.

Teach, E. (2003) Containing terrorism: Federal antiterrorism programs have spurred a sea change in supply-chain security, *CFO Magazine*, September, 87-90.

Tiebout, C.M. (1956) A pure theory of local expenditure, *Journal of Political Economy*,

United Nations Conference on Trade and Development (2003) *Review of Maritime Transport 2003*, New York: United Nations

US Customs and Border Protection (2004a) CSI Fact Sheet, Washington, DC: US CBP http://www.cbp.gov/linkhandler/cgov/enforcement/international_activities/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc Last Accessed 10 December 2004

US Customs and Border Protection (2004b) C-TPAT Fact Sheet and Frequently Asked Questions, Washington, DC: US CBP US http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fact_sheet.xml Last accessed 10 December 2004

US General Accounting Office (2002a) Critical infrastructure protection (CIP), testimony before the House of Representatives by Robert F. Dacey, Information Security Issues, GAO-02-961T. Washington: US General Accounting Office.

US Maritime Transportation Task Force (1999) *An Assessment of the US Marine Transportation System*, Washington DC: US Department of Transportation

World Shipping Council (2004) Liner Shipping: Facts and Figures. http://www.worldshipping.org/ind_facts.html Last accessed 10 December 2004.

World Trade Organization (2004) International Trade Statistics 2004, Geneva: WTO.