Bichou, Khalid

Working Paper

Security and risk-based models in shipping and ports: Review and critical analysis

OECD/ITF Joint Transport Research Centre Discussion Paper, No. 2008-20

Provided in Cooperation with:
International Transport Forum (ITF), OECD

Suggested Citation: Bichou, Khalid (2008) : Security and risk-based models in shipping and ports: Review and critical analysis, OECD/ITF Joint Transport Research Centre Discussion Paper, No. 2008-20, Organisation for Economic Co-operation and Development (OECD), Joint Transport Research Centre (JTRC), Paris, https://doi.org/10.1787/228863484281

This Version is available at:
https://hdl.handle.net/10419/68765

JOINT TRANSPORT RESEARCH CENTRE

Discussion Paper No. 2008-20
December 2008

Security and Risk-Based Models in Shipping and Ports: Review and Critical Analysis

Khalid BICHOU
Centre for Transport Studies
Imperial College London, United Kingdom

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

International Transport Forum

JOINT TRANSPORT RESEARCH CENTRE

Discussion Paper No. 2008-20

REVISED 2-12-08

Prepared for the OECD/ITF Round Table of 11-12 December 2008 on

Security, Risk Perception and Cost-Benefit Analysis

SECURITY AND RISK-BASED MODELS IN SHIPPING AND PORTS: REVIEW AND CRITICAL ANALYSIS

Khalid BICHOU

Centre for Transport Studies
Imperial College London
United Kingdom

December 2008

SECURITY AND RISK-BASED MODELS IN SHIPPING AND PORTS: REVIEW AND CRITICAL ANALYSIS

Revised 2-12-08

Khalid Bichou

Centre for Transport Studies, Imperial College London, UK

ABSTRACT

The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network. When managing risk through legislation, regulatory assessment models are used to assess risk levels and examine the impact of policy options, usually in terms of the costs and benefits of a regulatory proposal. This paper reviews the development, application and adequacy of existing risk assessment and management models to maritime and port security. In particular, we examine the problematical issues of security perception, value and impact, and discuss the limitations of the current regulatory framework in providing an integrated and effective approach to risk assessment and management, including for supply chain security.

1. OVERVIEW OF THE NEW SECURITY REGIME IN SHIPPING AND PORTS

Since the terrorist attacks in the US in September 2001 and with the growing concern about the security of the international movement of goods and passengers, several frameworks have been introduced either on a compulsory or voluntary basis with a view to enhancing maritime and port security. Regulatory measures that have been multilaterally endorsed and implemented include the International Ship and Port Facility Security (ISPS) code, the IMO/ILO code of practice on security in ports, and the World's Customs Organisation (WCO) 'Framework of Standards to Secure and Facilitate Global Trade' also referred to as 'SAFE Framework'.

A second set of security initiatives has been introduced at various national levels with the US led initiatives being the most significant. The US measures started with common initiatives such as the Maritime Transportation Act (MTSA) of 2002, which involves both mandatory and voluntary ISPS provisions (DHS, 2003), and later introduced a range of layered security programmes that target specific types of maritime operations. Major programmes under this category include the Container Security Initiative (CSI), the 24-hour Advanced Manifest Rule (hereafter referred to as the 24-hour rule), the Customs and Trade Partnership against Terrorism (C-TPAT), the Operation Safe Commerce (OSC), the mega-port initiative, and the Secure Freight Initiative (SFA). Except the 24-hour rule, these programmes and others have later been codified into the US Safe Port Act. Other national programmes include Canada's and Mexico's own 24-hour rules and the Swedish Stair-sec programme.

Initiatives have also emerged from the European Commission (EC) in the guise of the EC Regulation 725/2004 on enhancing ship and port facility security, Regulation 884/2005 laying down procedures for conducting Commission inspections in maritime security, and the Directive 2005/65/EC extending security measures from the ship-port interface to the entire port facility. The Authorised Economic Operator (AEO), the status and accreditation of which were introduced in the EU Custom Security Program implemented on January 1, 2008, is a scheme that deserves particular attention since it can be seen as the EU response to the US C-TAPAT programme. Outside the EU, regional initiatives that are worth mentioning include the US-Canada-Mexico Free and Secure Trade (FAST) initiative, the ASEAN/Japan Maritime Transport Security, and the Secure Trade in the APEC Region (STAR) for Asia Pacific. The Secured Export Partnership (SIP) is a bilateral customs security arrangement designed to protect cargo exported from New Zealand to the USA against tampering, sabotage, smuggling of terrorists or terrorist-related goods, and other transnational crime, from the point of packing to delivery.

A final set of security initiatives consists of primarily industry led and voluntary programmes. Initiatives under this category include the Secured Export Partnership (SEP) programme, the ISO/PAS 28000: 2005 standard (Specification for security management systems for the supply chain), the Business anti-Smuggling Coalition (BASC) scheme, the Technology Asset Protection Association (TAPA) initiative, and a series of Partnership in

Protection (PIP) arrangements. Although some of these programmes have not been fully implemented yet, it is believed that they will yield a more effective framework and a higher level of security assurance across and beyond the maritime network. For a detailed review and analysis of these initiatives and other port and maritime security measures, the reader is referred to Bichou et al. (2007a).

With such complexities in the current maritime security framework, much of the literature on the subject has focused on prescriptive details of the measures being put in place as well as on their *ex-ante* costs of compliance. However, there has been little work on security-risk assessment and management models, be it at the physical level or the supply chain level. In this paper, we review the development, application and adequacy of existing risk assessment and management models to maritime and port security. In particular, we examine current approaches to security-risk assessment and establish the link between physical security and supply chain security. However, not all aspects relevant to security-risk analysis in shipping and ports are discussed in this paper which limits the analysis to maritime reporting and precursor analysis, economic evaluation of regulatory measures, and alternative approaches of risk assessment and performance.

2. CONVENTIONAL RISK ASSESSMENT IN SHIPPING AND PORTS

2.1 System's Safety Approach to Risks and Hazard Analysis

The conventional approach to risk defines it as being the chance, in quantifiable terms, of an accident or adverse occurrence. It therefore combines a probabilistic measure of the occurrence of an event with a measure of the consequence, or impact, of that event. The process of risk assessment and management is generally based on three sets of sequenced and inter-related activities as outlined below.

- The assessment of risk in terms of what can go wrong, the probability of it going wrong, and the possible consequences,
- The management of risk in terms of what can be done, the options and trade-offs available between the costs, the benefits and the risks, and

- The impact of risk management decisions and policies on future options and undertakings.

Performing each set of activity requires multi-perspective analysis and modelling of all conceivable sources and impacts of risks as well as viable options for decision making and management. The empiricist approach is to regard accidents as *random events* whose frequency is influenced by certain factors. Under this approach, the immediate cause of an accident is known in the system safety literature as a hazardous event. A hazardous event has both causes and consequences. The sum of the consequences constitutes the size of the accident. Hazardous events range in frequency and severity from high frequency low consequence events (e.g. road accident or machine failure), which tend to be routine and well reported, to low frequency high consequence events (e.g. earthquake or terrorist attack), which tend to be rare but more complex.

Several analytical tools have been developed for hazard analysis. The choice of tool depends on (i) whether the causes or the consequences of a hazardous event are to be analysed, and on (ii) whether the techniques used take into consideration or not the sequence of the causes or consequences.

Table1. **Major Hazard Analysis tools**

	Consequence analysis	Cause analysis
Sequence dependent	Event Tree Analysis	Markov Process
Sequence independent	Failure Mode and Effects	Fault Tree Analysis

The causes of a hazardous event are usually represented by a fault tree which is a logical process that examines all potential incidents leading up to a critical incident. A popular methodology that relates the occurrence and sequence of different types of incidents is the fault tree analysis (FTA). Under the FTA, a mathematical model is fitted to past accident data in order to identify the most influential factors (top events) and estimate their effects on the accident rate. The model is then used to predict the likelihood of future accidents. The extent to which the tree is developed (from top to basic events) is usually governed by the availability of data with which to calculate the frequencies of the causes at the

extremities of the tree, so that these may be assigned likelihoods. From these, the likelihood of the top event is deduced.

FTA has a number of limitations. For instance, the approach assumes that the causes are random and statistically independent but certain common causes can lead to correlations in event probabilities which violate the independence assumptions and could exaggerate the likelihood of an event fault. In a similar vein, missed or unrecorded causes may equally bias the calculated likelihood of a hazardous event. Another shortcoming of the fault tree analysis is the assumption that the sequence of causes is not relevant. Where the sequence does matter, Markov-chain techniques may be applied.

The consequences of a hazardous event may be analysed using an event tree. Event tree analysis (ETA) is a logical process that works the opposite way of FTA by focusing on events that could occur after a critical incident. Under ETA, a statistical analysis of past accidents is performed to estimate the consequences of each type of accident in order to predict risk and consequences of future accidents. The event tree approach implies that the events following the initial accident, if they occur, follow a particular sequence. Where a particular sequence is not implied, 'Failure Modes and Effects' analysis may be used. This technique seeks to identify the different failure modes that could occur in a system and the effects that these failures would have on the system as a whole.

Most of the general tools described above have been successfully applied across many areas of maritime and port safety, with the Formal Safety Assessment (FSA) being the most standardised framework of risk analysis in regulated maritime systems. The FSA was first developed by the UK maritime and Coast Guard Agency (MCA) and later incorporated into the International Maritime Organisation (IMO) interim guidelines for safety assessment (IMO, 1997). The FSA methodology consists of a five-step process: hazards identification, risk assessment, risk management (alternative options), cost-benefit analysis, and decision making (MCA, 1996).

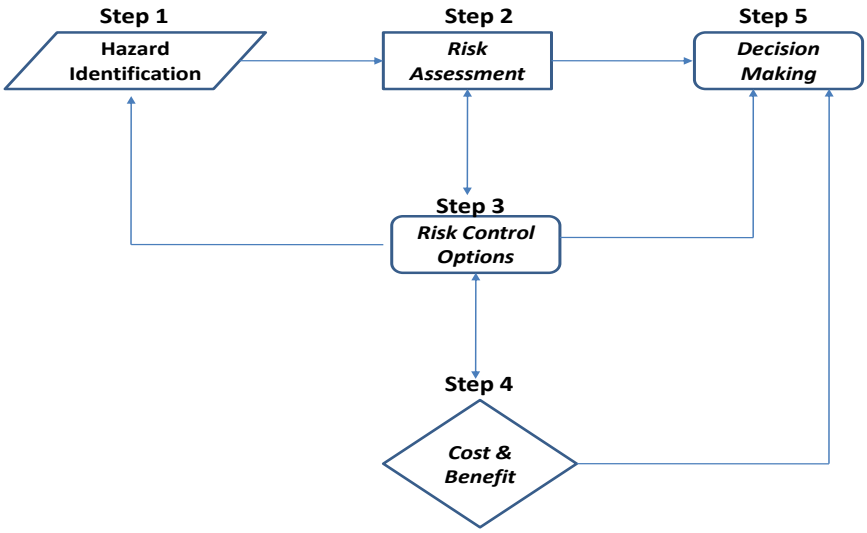


Figure 1: **FSA Methodology** (adapted by the author from MCA, 1996)

Despite the variety analytical tools available, the FSA and other conventional risk assessment models involve a substantial element of subjective judgement for both the causes and he consequences. The assumption of randomness of the causes of hazardous events is particularly problematic for low frequency high consequence events. The calculation of the consequences of an accident can also be subjective. Furthermore, any analytical tool for risk analysis requires that the boundaries, components, and functioning of the system is well established but this is not always evident in the context of shipping and port operations given the combination of several elements related to vehicle, facility, cargo, equipment, communication, labour and several environmental and exogenous factors.

2.2 The Current Risk Approach to Maritime Security

A typical example of maritime security risk models based on system's safety is the widely accepted Navigation Vessel Inspection Circular (NVIC) No. 11-02 "*Recommended Security Guidelines for Facilities*" published by the US Coast Guard. Under this circular, the risk-based framework for security assessment and management is structured in terms of 5 steps.

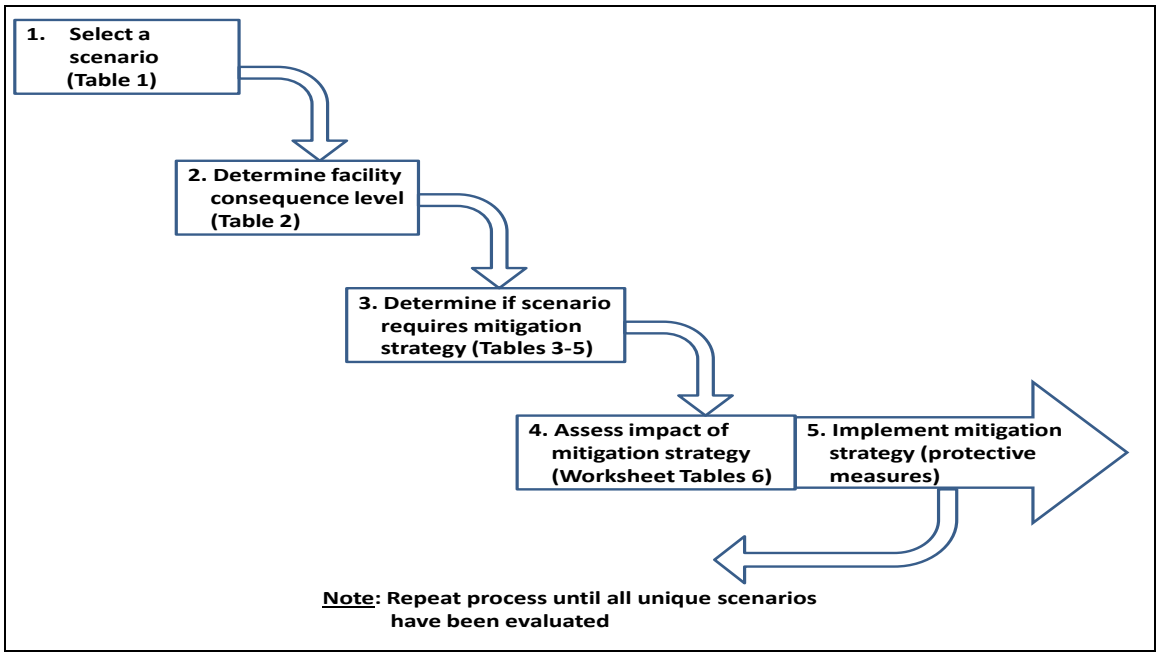


Figure 2: **The NVIC risk assessment model**

Step 1 of the risk-based assessment begins by selecting an attack scenario that consists of a potential threat to the vehicle (e.g. ship, truck), cargo/ passengers, facility (e.g. port, equipment), and/or operation (e.g. cargo handling). In the context of the maritime security regulatory regime, such scenarios must be consistent with scenarios developed for formal assessment models such as the ISPS provisions for ship security plan (SSP) or port-facility security plan (PFSP). Step 2 of the risk-based security assessment is to determine the appropriate consequence level for the type of activity on which the risk assessment is based. Step 3 refers to vulnerability assessment with four factors considered for vulnerability scoring: availability, accessibility, organic security and facility hardness. In the context of the ISPS Code, The NVIC grading scenario-risk method may be assimilated to the ISPS provisions of maritime security (MARSEC) levels ranging from (1) for minor to (3) for severe. An indication of vulnerability scores in the case of transportation and warehousing of bulk cargo is provided in table 3. Step 4 deals with the mitigation of the risk. As shown in table 4, this can be achieved by determining where the scenario falls based on the consequence level and vulnerability assessment score.

Table 2: **NVIC national list of scenarios**

Typical types of scenarios		Application example
Intrude and/or take control of the target and....	Damage/destroy the target with explosives	Intruder plants explosives
	Damage/destroy the target through malicious operations/acts	Intruder takes control of a facility internationally open valves to release oil or hazmat that may then be ignited.
	Create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release oil or toxic materials or release toxic material brought along.
	Take hostages/skills people	Goal of the intruder is to kill people
Externally attack the facility by...	Launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc. To damage or destroy bulk storage tanks, dangerous cargo, etc.
Use the facility as means of transferring...	Materials, contraband, and/or cash into/out of the country	Facility is used as conduit for *transportation security incident*
	People into/out of the country	

Table 3: **Vulnerability scenarios and scores**

Score	**Accessibility**	**Organic security**
3	No deterrence (e.g. unrestricted access to facility and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability.)
2	Fair deterrence (e.g. single substantial barrier, unrestricted access to within 100 yards of bulk storage tanks)	Fair deterrence capability (e.g. minimal security plan, some communications, security force of limited size relative to the facility, outside law enforcement with limited availability for timely prevention, limited detection systems)
1	Good deterrence (expected to deter attack, access restricted to within 500 yards of bulk storage tanks, multiple physical/geographical barriers)	Good deterrence capability expected to deter attack (e.g. detailed security plan, effective emergency communications, well trained and equipped security personnel, multiple detection systems (camera, x-ray, etc.), timely outside law enforcement for prevention.)

Table 4: **Vulnerability and Consequence Matrix**

	Total vulnerability score (Table 3)		
Consequence Level (Table 2)	**2**	**3-4**	**5-6**
	Consider	Mitigate	Mitigate
	Document	Consider	Mitigate
	Document	Document	Consider

3. SHORTCOMINGS OF CONVENTIONAL MODELS FOR ANALYSING MARITIME AND PORT SECURITY RISK

The NVIC model and other conventional risk models follow a safety-risk approach but the latter is based on the assumption of unintentional human and system behaviour to cause harm. This is not the case for security incidents stemming from terrorism or other malicious acts. Another major problem with assessing security threats is that much of the assessment process is intelligence-based, which does not always follow the scrutiny of statistical reasoning. Even with a sound intelligence risk approach, there are many uncertainties involved such as in terms of higher levels of noise in background data. An additional instance of inadequacy of conventional risk models to maritime security is the lack of historical data given the rarity of occurrence of large scale terrorist incidents. Another important issue stems from the supply chain dimension of the international shipping and port network, and as such data on the scope and levels of externalities are extremely difficult to extract and analyse. In either case, the security of the maritime network must be considered in both its physical and supply chain dimension, the latter evolving around disruptions and risk-driven uncertainties in the supply chain. In the followings, we discuss two main drawbacks of the current regulatory framework in relation with the assessment and management of the security risk for ships and shipping operations, namely: the inconsistencies in the current maritime reporting system and the failure to consider the supply chain dimension of security.

3.1 Reporting Systems and Maritime Security

3.1.1 Security incidents and precursor analysis

A broad definition of precursors may involve any internal or external condition, event, sequence, or any combination of these that precedes and ultimately leads to adverse events. More focused definitions reduce the range of precursors to specific conditions or limit their scope to a specified level of accident's outcome. For instance, the US nuclear regulatory commission (NRC) defines a precursor as *'any event that exceeds a specified level of severity'* (NRC, 1978), while other organisations incorporate a wider range of severities. In either case, a quantitative threshold may be established for the conditional probability of an incident given a certain precursor, with events of lesser severity being considered either as non-precursors with no further analysis or as non-precursors that need categorisation and further investigation.

Following the events of 11 September 2001, several formalised programmes have been developed for observing, analysing and managing accident precursors including comparison charts and reporting systems. In recent years, several organisations have designed and implemented reporting systems for security incidents/accidents with the most recognisable reporting system being the colour alert system used by the US Department of Homeland Security (DHS). Relevant examples in maritime security include the International Maritime Organisation (IMO) reporting system for ISPS compliance, International Maritime Bureau (IMB) reports of piracy accidents, and a number of voluntary reporting initiatives for maritime safety (BTS, 2002).

A major drawback resulting from the combination of warning thresholds and security event reporting is that the system may depict several flaws and errors. If vulnerabilities are defined too precisely or the threshold is set too high, several risk-significant events may not be reported. On the other hand, setting the threshold for reporting too low may overwhelm the system by depicting many false alarms, and ultimately a loss of trust in the system. Table 5 shows the types of errors that may occur given these conflicting approaches. Type I error refers to a false negative and occurs in situations of missed signals when an accident occurs with no warning being issued. Type II error refers to false

positive whereby a false alert is issued, leading for instance to mass evacuation or a general disturbance of the system.

Table 5: **Errors resulting from the interplay between threshold settings and event reporting**

	Significant	Not significant
Event reported	True positive (Significant event)	False positive (Type II error)
Event not reported	False negative (Type I error)	True negative (Non-significant event)

Another issue arising from reporting security precursors under regulatory constraints relates to the fact that reported data remains in the hands of the regulator. This raises questions about (i) the reliability and validity of information since fears of regulatory actions may discourage organisations from reporting precursor events and (ii) the dissemination of reported information given that the regulator may restrict access to data which is considered too sensitive to be shared. The argument here is that the purpose of reporting must emphasise organisational learning along with a guarantee of privacy and immunity from penalties for those reporting the information.

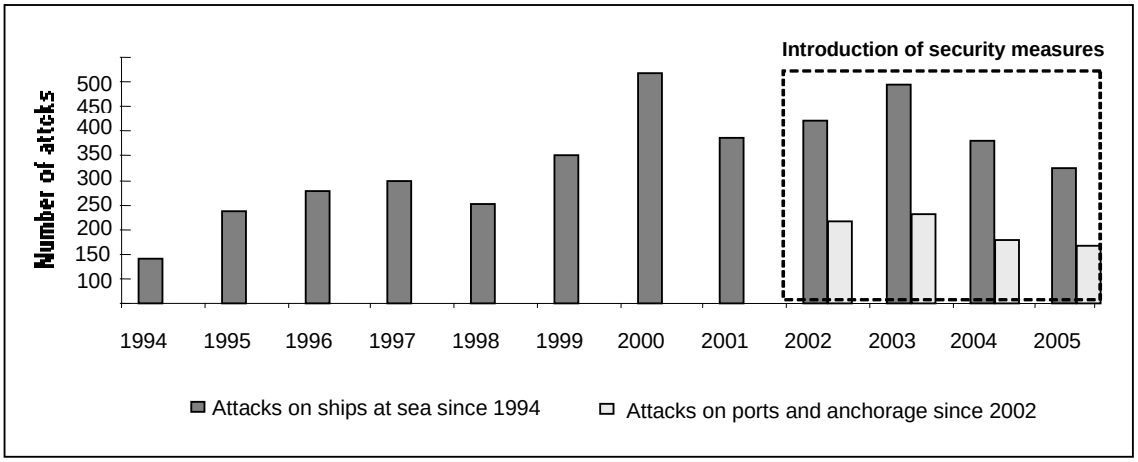
A particular aspect of precursor analysis is the so-called 'near miss' also referred to as the near hit, the close call, or simply the incident. A near miss is similar to an accident except that it does not necessarily result in injury or damage. It is a particular kind of precursor with elements that can be observed in isolation without the occurrence of an accident. The advantage of the concept is that organisations with little or no history of major incidents can establish systems for reporting and analysing near misses. This is because it has been found that near misses occur with greater frequency than the actual event (Bird and Germain, 1996). This argument is even made stronger with much of the literature on reported transport accidents confirming that near misses have usually preceded the actual incidents (Cullen, 2000; BEA, 2002).

In maritime security, implementing programmes of security assessment based on precursor analysis would have a number of benefits including for such aspects as

identifying unknown failure modes and analysing the effectiveness of actions taken to reduce risk. Another opportunity from precursor analysis is the development of trends in reported data, which may be used for the purpose of risk management and mitigation. Even though, there is no formal categorisation between incident and accident reporting in shipping and ports. Furthermore, we are not aware of any formal precursor programme being implemented in the context of maritime security, except for on-going research into potential security hazards for liquid-bulk and specialised ships such as LNG and LPG vessels. On the one hand, inherently secure designs against the threats of terrorism and other similar acts are yet to be developed, although improvements have been made in ship design for safer and sustainable transportation. On the other hand, existing reporting schemes of maritime security incidents noticeable gaps in both content and methodology. This is the case for instance for piracy and armed robbery incidents whereby available reports show general information with no sufficiently detailed data to display and analyse incident precursors (See table 6), although the recent piracy incidents in the Gulf of Aden may trigger a radical change in piracy-incident reporting.

Table 6: **Reported actual and attempted piracy incidents on ships and ports**

(Compiled by the author from IMB & IMO annual piracy reports)



Analysis of accident precursors can also be useful in conjunction with probabilistic risk analysis (PRA). PRA is a quantitative risk assessment method for estimating risk failure based on system's process mapping and decomposition into components (Bier, 1993; Bedford and Cook, 2001). PRA has been used in a variety of applications including risk analysis in transportation systems. PRA can be combined with precursor analysis to

quantify the probability of accidents given a certain precursor, thus helping in prioritising precursors for further analysis or corrective actions. The method can also be improved based on precursor data analysis such as by checking on the validity of PRA model assumptions. An instance of modelling port operations for the purpose of PRA and accident precursor analysis is provided in Figure 3 below.

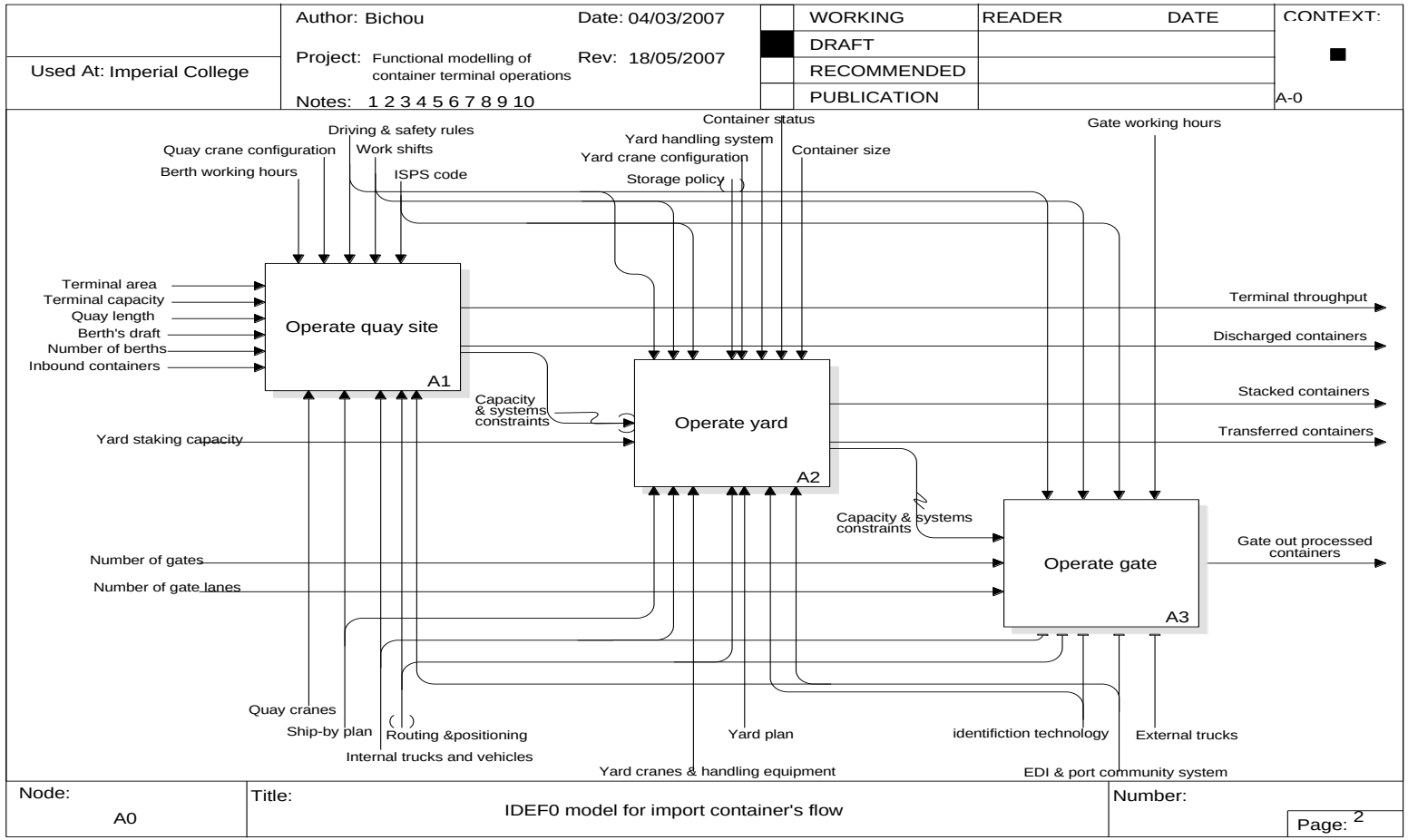


Figure 3: **A model of import container's flow for PRA and precursor analysis**
(Source: Author)

3.1.2 Shipping security and reporting procedures

One of major the changes brought about by maritime and shipping security is that further documentation and screening for the cargo being transported by sea is now required. Even though, such requirements are not always consistent between regulations or countries. An instance of anomalies in maritime reporting and documentation systems is when ships and their cargoes become exempt from regular customs inspections when sailing between ports of countries belonging to the same trading or economic block such as the EU or NAFTA. In the EU for example, Member States of the European Union enjoy the freedom of moving goods within the Community, which means that as long as consignments originate within the EU, there are no controls concerning their movement. The issue of the exemption of Authorised Regular Shipping Services from Customs Reporting Regimes gives rise to anomalies in the reporting of cargoes, as it is very likely that such vessels are not only carrying goods of EU Origin but also consignments under Community Transit Customs control, or sometimes cargo originating from outside the EU. Unless that cargo is individually reported as being in separate containers or trailers, or the vessel itself is registered within the EU, the cargo may not be declared and its content may be unclear. Vessels sailing in EU territorial waters may also be carrying consignments on a consolidated basis and for which there is only brief summary details referring to the consolidation, and not necessarily for each individual grouped consignment.

To avoid such anomalies, countries such as the USA have introduced detailed documentation and reporting systems such as through the 24-hour rule. However, because of the requirements of such levels of details under the new security regulations, shipping lines and their agents may fail to produce the relevant documentation and related detailed cargo description so as to conform to the 24-hour rule and other maritime security requirements. A sample of potential errors that might occur in the work processes while satisfying maritime security is provided in table 7.

Even with detailed procedural regulations such as the 24-hour rule, full and accurate information regarding cargo movement and ownership throughout the supply chain may not be readily available to regulators or customs authorities. This is typically the case when using a combination of transport modes (multimodal transportation) and consolidation

arrangements. For the latter, the description of Less-than-Container-Load (LCL) consignments in terms such as “Said to Contain” or “Freight of all Kinds” (FAK) creates a vacuum in information transparency and accessibility as far as the carriage of goods on groupage consignment is concerned. A more radical example is that of a consignment described loosely as “Cosmetic Products”, which may contain commodities ranging from aromatic oils through soaps to lipsticks and nail varnish. However, the consignment may also include items such as nail varnish remover, which is classed as Hazardous Goods because of its flammable nature, but since the overall groupage consignment description made no mention of this, the specific commodity was overlooked and no specific Dangerous Goods documentation was issued for the nail varnish remover, despite the evident risk involved in the shipment of the consignment.

Table 7: **Potential errors from implementing the 24-hour rule**

(Source: Bichou et. al, 2007)

Functional department	**Potential errors**
Marketing	Flagging the CSI cargo in business information system Booking data quality Booking Confirmation to shipper CSI cut-off time
Administration (documentation and ICT)	Manifest data quality Transmission of manifest data to AMS timely Handling amendment Bill of Lading issuance to shipper Rating the shipment Billing the CSI fee and amendment fee
Operations	Ship/ port planning Release of empty container Coordination with terminals & customers for cargo inspection

The nature of the international supply chain demands that information pertaining to cargoes is passed down the line from Supplier to Customer in order to ensure the smooth and efficient despatch and delivery of the consignment, and that all authorities and parties within the supply chain, especially from a transportation and national control perspective,

are fully informed as to the nature and risk of the consignment in question. Even when no international frontier controls are involved, such as within the European Union, there is still a significant need for such flows of information especially where combined forms of transport are involved. This issue will be examined further in the next section.

A further issue arising from the new requirement for detailed reporting stems from the on-going trend of increase in vessel size. For instance, the wide deployment of new Super Post-Panamax container vessels means that the Cargo Manifest for each vessel becomes larger, with the risk that the computer systems required to analyse the information therein require updating to cover the increased volume of information or may take some time to absorb all the information contained therein. Given the sheer volume of container information in each manifest, it is too cumbersome a task for the Customs Computer or the Customs Officer to analyse each cargo at the time the manifest is submitted, although containers are selected at random for scanning and examination at the port.

Last, but not least, the issue of container security poses problem as there are yet no agreed international standards and regulations on the enforcement of container seals (mechanical and electronic) used in international transport movements. Container security consists of a complex system of interrelated activities in information and data capture, physical surveillance of the container, and inquiries into the various actors in the supply chain; but any standardisation process must decide on the privacy of the parties involved and their wiliness to share information between each other.

3.2 The Supply Chain Risk Dimension of Maritime Security

Since the introduction of the new security regime in shipping and ports, researchers and practitioners alike have questioned the wisdom of such plethora of regulations. Others have justified the overlap of these programmes by the need to establish a multi-layer regulatory system in an effort to fill potential security gaps (Flynn, 2004; Willis and Ortiz, 2004). The concept of layered security is not entirely new to transport systems and dates back to the 1970s. Prior to the introduction of new maritime security measures, the concept has also been cited in 1997 in the context of aviation security (Gore Commission, 1997).

To illustrate the application of the layered approach to maritime and supply chain security, we develop a conceptual construct of the structure and functioning of the international maritime network. The system is portrayed in terms of three chains or channels (logistics, trade and supply) and three flows (payment, information, and physical). A chain or channel is a pathway tracing the movement of a cargo-shipment across a 'typology' of multi-institutional and cross-functional alignments, while flows are the derived interactions or transactions between various 'functional institutions' within each channel. The logistics channel consists primarily of 3rd party specialists (ports, carriers, freight forwarders, 3PLs, 4PLs, etc.) that do not own the cargo but facilitate its efficient movement progress, for example through transportation, cargo handling, storage and warehousing. Both the trade channel and supply channel are associated with the ownership of goods moving through the system, with the difference that the trade channel is normally perceived to be at the level of the trade or the nation (e.g. the oil trade, the containerised trade, the US-Canada trade, the intra EU trade) and the supply channel at the level of the firm (e.g. Toyota and Wall-Mart supply chains, respectively). For each channel, one or a combination of physical, information and payment flows is taking place. Figure 4 depicts the interactions between channels and flows in a typical international maritime network.

As a justification of the need for a layered framework to port and maritime security, consider a typical global movement of a containerised cargo, which is estimated to involve as many as 25 parties and a compound number of flow-configurations within and across the supply chain network. Because of the increased trend of outsourcing and contract logistics, the role and scope of control exercised by members of the supply channel (mainly manufacturers, shippers and receivers) would only be limited oversee the management of direct interactions between them rather than the details of logistical arrangements. Arrangements such as cargo consolidation and break bulk, multi-modal combinations, transhipment and reverse logistics are typically performed by third parties including s, ports and other intermediaries. In a similar vein, the trade channel stakeholders (regulators, customs, health authorities, etc.) may be able to scrutinise and monitor the logistical segment within their own national territory, but would have little or no control over arrangements taking place in a foreign country including at transit and transhipment locations. Thus, the combination of intersecting functional and institutional arrangements

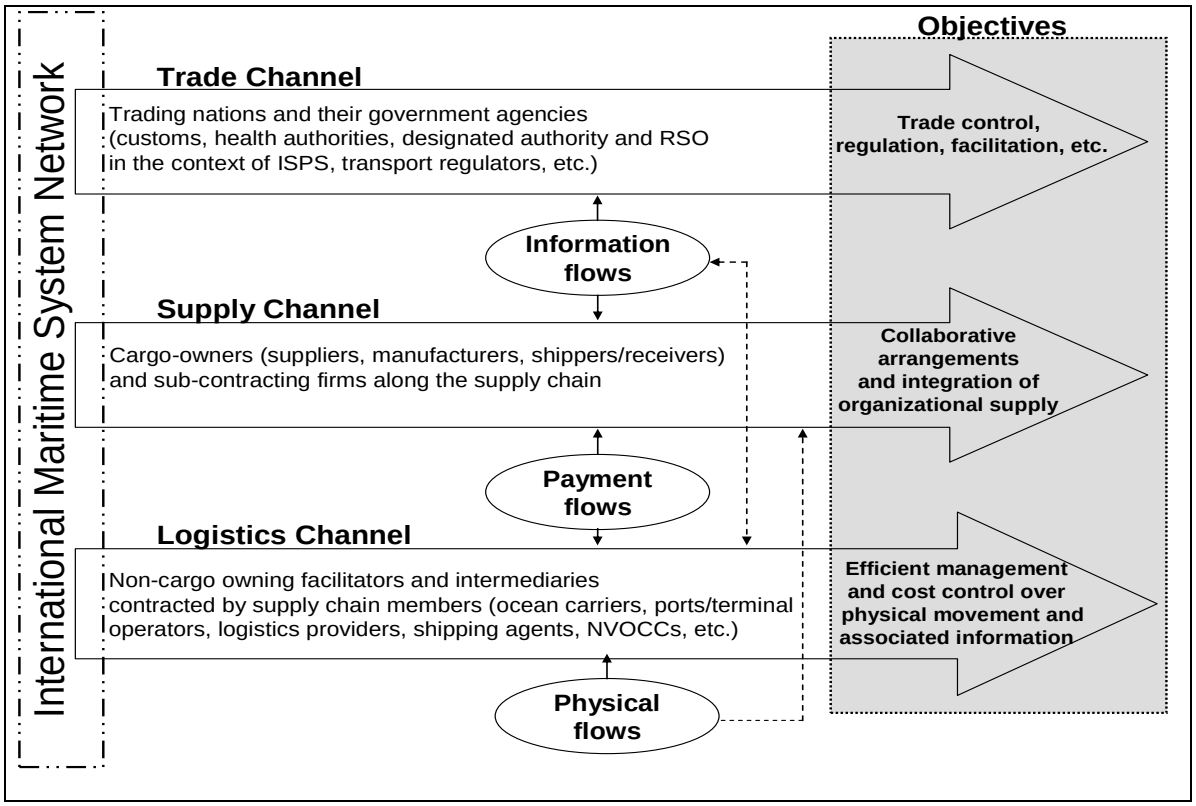


Figure 4: **Channel typologies and components of the maritime network**
(Bichou, 2007b)

across the supply chain makes it almost impossible for a single actor within a single channel, to effectively trace and monitor every cargo movement and operation across different channels. This largely explains the use of multi-channel layered approach to monitor the security of maritime and port operations, for instance through regulations such as the CSI and the 24-hour rule. Figure 4 depicts the hierarchy of regulatory programmes by level of security and supply chain coverage. The levels relative to each programme are hypothetical but typical.

One can argue however that the layered approach, as being currently implemented, has not yet materialised into an integrated and comprehensive system capable of overcoming existing and potential security gaps. For instance, the emphasis on goods and passenger movements has diverted the attention away from non-physical movements such as financial and information flows. The latter involve the use of a range of communication systems including radar systems and electronic data interchange (EDI); but no agreed procedure on ensuring the security of such systems as well as on related data security in

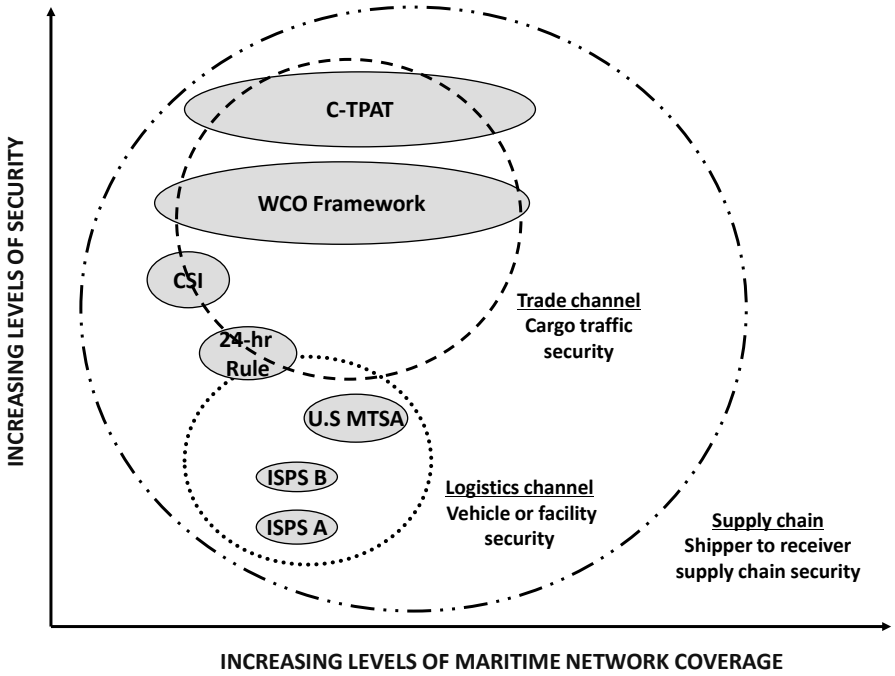


Figure 5: **Hierarchy of security measures by level of security and network coverage** (Bichou, 2005)

the context of maritime operations has been incorporated in the current maritime security framework. Other security gaps include the exclusion from the current regulatory regime of fishing vessels, pleasure crafts and yachts, and other commercial ships of less-than 500 GT. There is also a lack of harmonisation between the new security regime and other maritime environmental and safety programmes such as the STCW convention and the ISM and IMDG codes.

Another aspect of interest when examining maritime network security is the interplay between supply chain security and supply chain risk, the latter being closely related to uncertainties stemming from specific supply chain configurations. Juttiner et al. (2003) review the literature on supply chain risk management and categorise sources of supply chain risk into three major groups:

- Environmental risk sources corresponding to uncertainties associated with external sources such as terrorism or environmental risks,
- Organisational risk sources relating to internal uncertainties within the supply chain , for instance strikes or production failures, and

- Network-related risk sources referring to uncertainties arising from the interactions between organisations in the supply chain.

The current maritime security framework strongly emphasises environmental and organisational risk sources, but there is less focus on network-related vulnerabilities. However, excluding or minimising network-related risk sources may overlook the capacity of the system to either absorb or amplify the impact of events arising from environmental or organisational sources. Examples of network-related risk drivers in maritime security include uncertainties caused by contracting with non-compliant (non-certified) supply chain partners. A recent study involving 20 top US firms has shown that there is a tendency among American shippers towards trading off lowest bidders with known suppliers (MIT/CTS interim report, 2003). There have been similar examples across the shipping and port industry, for instance shipping lines changing their ports of call because of the existence or absence of a regulatory programme.

4 ECONOMIC EVALUATION AND APPRAISAL OF MARITIME SECURITY MEASURES

In view of the new security regime, maritime operators have had to implement security measures in order to comply with security initiatives and the route to compliance frequently requires investment in security equipment, procedures and the recruitment and training of security personnel. In addition to the cost of compliance, port operators and users alike may incur extra costs stemming from the implementation of new procedural security and the provisions for detailed reporting, further inspections, and other operational requirements. Therefore, the literature on cost impacts of maritime security may be classified into two main categories: the literature on compliance costs and the literature on procedural and operational costs.

4.1 Compliance Cost of Port Security

4.1.1 Ex-ante assessment

Even before the entry in force of the new security regulations, several studies have attempted to assess the compliance cost of port security, particularly for formal security regulations such as the ISPS code. *Ex-ante* assessments of the compliance cost of

maritime and port security are largely based on data and methods from national regulatory risk assessment models such as the US National Risk Assessment Tool (N-RAT) and the UK Risk Assessment Exercise (RAE). These are ad-hoc programmes undertaken by governmental agencies in order to assess the costs and benefits of new regulatory initiatives. For instance, the US Coast Guard (USCG) has estimated the ISPS compliance cost for US ports to reach USD $1.1 billion for the first year and USD $656 million each year up to 2012. Based on these estimates, the Organisation for Economic Co-operation and Development (OECD, 2003) has produced a comprehensive report on the global economic impacts of maritime security measures. A summary of aggregate *ex-ante* estimates for ISPS cost-compliance is provided in Table 8. Regarding non-ISPS initiatives, a study funded by the European Commission (EC) suggests that voluntary security programmes, based on a participation level of 30% of European Union (EU) operators, would cost port and terminal operators in the EU around €5 Million just for audit expenses (DNV Consulting, 2005).

Table 8: **Summary of ISPS ex-ante cost estimates as computed by various regulatory risk assessment impacts**

Source of estimates	Cost items	Scope	Initial Costs*	Annual Costs*	Total cost* over 10 years (2003-13) @ 7% DFC
USCG	Total ISPS US ports	226 port authorities, of which 5000 facilities are computed (from Fairplay) (ISPS Parts A & B MARSEC Level 1)	1125	656	5399
	Total ISPS US-SOLAS and non-SOLAS vessels subject to the regulation	3500 US-flag vessels, as well as domestic and foreign non-SOLAS vessels (i.e. operating in US waters) (ISPS Parts A & B MARSEC Level 1)	218	176	1368
	Automated Identification System		30	1	50
	Maritime Area (contracting government)	47 COTP US zones	120 (+106 for 2004)	46	477
	OSC facility (offshore installations)	40 U.S OCS Facilities under US jurisdiction	3	5	37
	U.S cost for ISPS implementation	**(ISPS parts A and B)**	**115**	**884**	**7331**
	Aggregate Cost of elevating MARSEC level from 1 to 2	Based on a twice MARSEC level 2 per annum, each for 21 days	16 per day		
UK	Total ISPS UK port facilities	430 facilities (ISPS Part A MARSEC Level 1)	26	2.5	
	Total ISPS UK-flagged ships and company related costs	620 UK-flag vessels (ISPS Parts A, MARSEC Level 1) (Calculations based on an exchange rate of UK= £1.6 USD	7.4	5.2	
OECD	AIS	Based on 43,291 international commercial fleet of more than 1,000 GT (Passenger and cruise vessels not included), MARESC Level 1, ISPS Part A only	649.3	Undetermined	
	Other vessel measures		115.11	14.6	
	Ship operating companies		1163.89	715.4	
	Total ships & shipping companies		**1279**	**730**	
	PFSA, PFSA, PFSP	2,180 port authorities worldwide, of which 6,500 facilities are computed (from Fairplay) (ISPS Part A only MARSEC Level 1)	390.8	336.6	
	Total ISPS ports		Undetermined	Undetermined	
	Global cost for ISPS implementation	(MARESC level 1, ISPS part A only)	Undetermined	Undetermined	
Australian Government	Total costs for Australia	70 Australian flag ships and 70 ports, of which 300 port facilities	240 AUD	74 AUD	
Shipowners' association	Total costs for vessels	47 Australian vessels	29655 AUD		

*: All cost figures are expressed in 2003 USD $ million, except for Australia where costs are expressed in 2002 AUD $ million

Legend

AIS: Automated Information System, AUD: Australian Dollar, COTP: Captain of the Port, DFC: Discount Factor, GT: Gross tons, MARSEC: Maritime Security Level, OSC: Outer Continental Shelf, PFSA: Port Facility Security Assessment, PFSO: Port Facility Security Officer, PFSP: Port Facility Security Plan, SOLAS: The IMO International Convention on the Safety of Life at Sea

(Source: Bichou, 2005b)

4.1.2 Ex-post assessment

Following the entry into force and implementation of the new security measures, a number of *ex-post* assessments of the cost of compliance have been undertaken. In so doing, researchers have used a variety of approaches ranging from survey inquiries and economic impact studies to financial appraisal and insurance risk modelling:

- Among the plethora of survey inquiries on the subject, it is worth mentioning the United Nations Conference on Trade and Development (UNCTAD) global survey on initial and annual costs of ISPS compliance. The survey results suggest that for each ton or TEU handled, the average cost for ISPS compliance would amount USD $0.08 and $3.6 respectively, of which $0.03 and $2 in terms for annual (recurrent) costs respectively (UNCTAD, 2007). However, a recent survey by the World Bank found that the average ISPS compliance costs amount to $0.22 per ton and $4.95 per TEU handled (Kruk and Donner, 2008). Such contradictory findings may be explained by the variety of methods used to calculate the ISPS costs (unit versus average, initial versus running, etc.), but can also stem from the different interpretations of the Code across world ports and terminals (Bichou, 2004; Bosk, 2006). While the ISPS Code provides general provisions on security requirements in ports, it does not prescribe detailed and uniform instructions on how to comply with them, for instance in terms of the exact instructions on the type and height of fences required for each port or terminal facility.

- Another problem with survey inquiries occurs when the findings of a case-specific survey are generalised to all stakeholders and/or security programmes. For instance, Thibault et al. (2006) found that small ocean carriers generally enjoy lesser initial compliance costs but incur higher recurrent costs because of the difficulty to spread fixed costs across a small business base. However, Brooks and Button (2006) found that the costs of enhanced maritime and supply chain security only accounts for 1% or less of shippers' total costs. Even when survey inquiries investigate a single security programme, their results may show inconsistent cost figures either over time or between participants. For example, when first enrolments in the C-TPAT programme began in 2004, the industry widely quoted Hasbo's figures of USD $200,000 initial costs and USD $113,000 annual operating costs as being the benchmark for C-TPAT average compliance cost for a

multinational firm (Googley, 2004). However, in a recent survey of 1756 C-TAPAT certified participants, Diop et al. (2007) report that C-TPAT implementation and operating costs only amount to USD $38,471 and $69,000 USD, respectively. Furthermore, according to the same survey 33% of respondents said that the benefits of C-TPAT participation outweighed the costs while an additional 25% found that the CTPAT costs and benefits were about the same. Other surveys on the subject also provide contradictory results -see Lloyd's List (2003) and BDP (2004).

- As with survey inquiries, economic impact studies on the cost of port and maritime security also depict inconsistent results. For example, Damas (2001) estimated that the new security measures introduced in the awake of the 9/11 terrorist attacks would cost the US economy as much as USD $151 billion annually, of which USD $65 billion just for logistical changes to supply chains. However, a study undertaken by the International Monetary Fund in the same year has estimated the increase to business costs due to higher security costs to cost around USD $1.6 billion per year, with an extra financing burden of carrying 10% higher inventories at $7.5 billion per year (IMF, 2001). Such discrepancies are also observable in studies seeking to quantify the economic and supply chain cost of port security incidents and other similar disruptions such as industrial actions and natural disasters. For instance, Martin Associates (2001) estimated that the cost of US West-Coast port lockout in 2001 to the US economy to reach USD $1.94 billion a day, based on a 10-day shutdown of port facilities. However, by the time the labour dispute was resolved, Anderson (2002) priced the total economic cost at around USD $1.7 billion, based on a longer shutdown period of 12 days.

- Other researchers have looked at the knock-on effect of US ports' closure on other dependent economies and foreign ports. For example, Saywell and Borsuk (2002) estimated the loss from this disruption be as high as 1.1% of the combined GDP of Hong Kong, Singapore and Malaysia. In a similar vein, Booz Allen Hamilton (2002) run a port security war game simulation to assess the impacts of a terrorist incident in a US port followed by a nation-wide port and border-crossing closure for 8 days. With an estimated cost of USD $50 billion on the US economy, their results show inconsistent results with those of previous studies. Pritchard (2002) Zuckerman (2002) suggest even lower costs than those reported above.

- Cost assessment of regulatory initiatives may also be undertaken through financial and insurance risk modelling. For the former, ex-post costs are typically assessed by analysing market response to risk-return performance, for instance by translating security provisions into port investments and analysing their ex-post impact using models and techniques of financial appraisal and risk analysis. For the latter, researchers typically use premium-price analysis whereby security costs and benefits are added to or subtracted from the price of port and shipping services; referring inter-alia to the variations in freight rates and insurance premiums. For instance, Richardson (2004) reports that insurance premiums trebled for ships calling at Yemeni ports after the 2002 terrorist attack on the oil tanker *Limburg* off the Yemeni coast, which has also forced many ships to cut Yemen from their schedules or divert to ports in neighbouring states.

- Trade facilitation studies can also been used to analyse the ex-post impacts of security such as by measuring the time factor (delay or speed-up) brought by security measures. Nevertheless, despite the rich literature on the interface between trade facilitation and economic development (Hummels, 2001; Wilson et al., 2003), few studies have investigated the role of the new security regime as either a barrier or an incentive to trade (Raven, 2001). For instance, the OECD (2002) reports that post 9/11 trade security measures would have cost from 1% to 3% of North American trade flows corresponding to a cost between USD $60 billion and USD $180 billion in 2001 figures. Another estimate places the global costs for trade of post 9/11 tighter security at about USD $75 billion per year (Walkenhorst and Dihel, 2002).

- Another way for analysing the cost-benefit of a regulatory change is to contrast transfer costs against efficiency costs. The former refer to the costs incurred and recovered by market players through transferring them to final customers (e.g. from ports to ocean carriers or from ocean carriers to shippers), while the latter represent net losses and benefits in consumer and producer surpluses. Compiled cost figures from industry and press reports suggest an average security charge of USD $6 per shipped container, and up to USD $40 per bill of lading for the 24-hour rule. Note that this approach is not without bias, including the common practice of cost spin-off and exponential computations of security expenses. In a highly disintegrated and fragmented maritime and logistics industry, there is no guarantee that additional security charges accurately reflect the true incremental costs incurred by each operator, including ports. Standard practices in the

industry suggest that market players try to generate extra profits by transferring costs to each other (Evers and Johnson, 2000; Fung et. al, 2003), and there is already evidence of similar practices in the recovering of security costs by the port industry (see Table 9).

Table 9: Sample of container ports' security charges
(Source: Compiled by the Author from various trade journals)

Port or terminal			Security fee USD ($)/TEU
Europe	Belgian ports		10.98
	France and Denmark		6.1
	Dutch ports		10.37
	Italian ports		9.76
	Latvian ports		7.32
	Norwegian ports		2.44
	Spanish ports		6.1
	Irish ports		8.54
	Swedish ports (Gothenburg)		2.6
	UK ports	Felixstowe, Harwich and Thames port	19 for import and 10 for export
		Tilbury	12.7
USA	Charleston, Houston and Miami		5
	Gulf seaports marine terminal conference		2
Others	Shenzhen (China)		6.25

4.2 Procedural and Operational Impacts

The increasing interest into procedural and operational impacts of security has been fed largely by the continuing debate between those who anticipate productivity losses because of operational redundancies and those who advocate higher operational efficiency due to better procedural arrangements:

- On the one hand, many argue that procedural requirements of the new security regime act against operational and logistical efficiency. Proponents of this standpoint list a number of potential inefficiencies ranging from direct operational redundancies, such as lengthy procedures and further inspections, to derived supply chain disruptions such as in terms of longer lead times, higher inventory levels, and less reliable demand and supply scenarios. The 24-hour rule provides a typical example of procedural requirements with potential negative impacts on operational and logistics efficiencies. For example, the requirements of the 24-hour will result in ocean carriers declining any late shipment bookings but also bearing, under customary arrangements, the cost of at least one extra day of container idle time at ports. The latter may be extended to three days or more for carriers and forwarders that are not electronically hooked into the US CBP Automated Manifest System (AMS). Shippers and receivers alike will then have to adjust their production, distribution and inventory management processes accordingly. Ports will also bear commercial and cost impacts of the 24-hour rule, including potential congestion problems and possible delays in both ships' departures and arrivals. Additional costs to shippers may also stem from the extra time and resources needed for carriers to compile and record detailed data information. In fact, shipping lines have already started transferring the cost of the 24-hour rule data filing and processing requirements to shippers and cargo owners who now have to pay an extra USD $40 levying charge per bill of lading (Lloyd's List, 2003), plus any additional indirect costs from advanced cut-off times and changes in production and distribution processes. Ocean carriers and NVOCCs may also be faced with a violation fine of USD $5000 for the first time and USD $10000 thereafter in case they submit missing or inaccurate data to CBP. A detailed review of the 24-hour requirements, costs, and benefits is provided by Bichou et al. (2007a).

- On the other hand, proponents of new security measures argue that their implementation is not only necessary but can also be commercially rewarding. The main argument put forward is that measures such as the CSI, the 24-hour rule and the C-TPAT fundamentally shift the focus from inspection to prevention, the benefit of which offsets and ultimately outweighs initial and recurrent costs of implementation. Detailed data recording, electronic reporting and other procedural requirements brought about by the new security regulations would allow for pre-screening and deliberate targeting of 'suspected' containers, which is proven as more cost-effective and less time-consuming than the traditional approach of random physical inspections. In addition to the benefits of access

certification and fast-lane treatment, compliant participants would also benefit from reduced insurance costs, penalties and risk exposure. Other advantages that go beyond the intended security benefits include the protection of legitimate commerce, the exposure of revenue evasion, reduced risk of cargo theft and pilferage, real-time sharing of shipping and port intelligence, advanced cargo processing procedures, and improved lead-time predictability and supply chain visibility.

Nevertheless, both arguments are rarely supported by empirical analysis and much of analytical research on procedural security impacts uses modelling techniques to predict the operational costs and benefits of security. Lee and Whang (2005) have developed a mathematical model to assess the benefits of reduced lead times and inspection levels in the context of Smart and Secure Trade-lanes (SST). White (2002) also used mathematical modelling by developing a min-depth heuristic to minimise the number of container moves in the case of CSI. Using simulation, Babione et al. (2003) examined the impacts of selected security initiatives on import and export container traffic of the port of Seattle. Rabadi et al. (2007) used a discrete event simulation model to investigate the impact of security incidents on recovery cycle for the US container terminal of Virginia. Other simulators have been specifically designed to run pre-defined disruption scenarios and predict their impacts on port efficiency. For example, the national infrastructure simulation and analysis centre (NISAC) has developed two port simulators, an operations simulator to evaluate the short-term operational impacts and an economic simulator to assess long-term economic impacts (NISAC, 2005).

4.3 CBA and Maritime Security

In evaluating the costs and benefits for optimal regulatory decisions, cost-benefit analysis (CBA) is regarded as a fairly objective method of making assessments. Cost-efficiency analysis (CEA) is an alternative method to CBA usually applied when the output is fixed and the economic benefits cannot be expressed in monetary terms. CBA and CEA are widely used to assess the efficiency of various measures and alternatives such as in terms of a new regulatory regime or a new investment (e.g. in infrastructure or technology). In the context of maritime regulation, CBA is a key component of the FSA methodology and other formal assessment procedures.

However, in a typical CBA or CEA model the results of implementing a regulation can be entirely different from one stakeholder (firm, nation-state, etc.) to another. The concept of externality is very difficult to apprehend in the context of malicious incidents. According to the definition of externality, costs arising from accidents are external when one person or entity causes harm to another person involved in the accident, or a third party, without providing appropriate compensation. Risk decisions regarding the introduction of regulatory measures involve multiple stakeholders who influence decisions through a complex set of legal and deliberative processes. Whether this is beneficial to the whole community or not is very debatable given the differences between stakeholders' values and perspectives. In a typically fragmented maritime industry, this focus raises the important question: costs or benefits to whom? In other words, who will bear the cost of or gain the benefits from the compliance with statutory measures.

To correct CBA/CEA deficiencies particularly with regard to cost sharing and distribution, Stakeholder Analysis (SHA) was introduced in the early 1980s. SHA is designed to identify the key players (stakeholders) of a project or a regulation, and assess their interests and power differentials for the purpose of project formulation and impact analysis. Several procedures have been proposed for SHA implementation, with the World Bank four-step formula (stakeholders identification, stakeholders interests, power and influence inter-relationships, and strategy formulation) being the most recognised and widely used. It must be noted however that there is no clear-cut predominance of a method over another, and quite often not all the conditions for the implementation of a complete regulatory assessment exercise are met.

An important element in any valuation method of new regulatory decisions is the cost of preventing principal losses in security incidents, a key component of which stems from human casualties, that is fatalities and injuries. However, since the value of these losses is not observable in market transactions, most economists believe that these valuations should be based on the preferences of those who benefit from security measures and who also pay for them, either directly or through taxation. In the context of casualty prevention, these preferences are often measured using the ‘willingness to pay’ (WTP) approach, that is the amount people or society is willing to pay to reduce the risk of death or injury before the events. There are two major empirical approaches to estimating WTP values for risk

reductions, namely the revealed preference method (RPM) and the stated preference method (SPM). RPM involves identifying situations where people (or society) do actually trade off money against risk, such as when they may buy safety (or security) measures or when they may take more or less risky jobs for more or less wages. SPM on the other hand involves asking people more or less directly about their hypothetical willingness to pay for safety/security measures that give them specified reductions in risk in specified contexts. The WTP approach has been extensively used in the context of road safety, but little literature exists on the use of the methodology in the context of shipping safety, let alone in the context of maritime and port security. The problem with the WTP approach in the latter context is that it is difficult to assume that people or society are capable of estimating the risks they face from terrorism (RPM) or that they are willing to answer questions about trading-off their security, or safety, against a given amount of money (SPM).

5 CONCLUSION

This paper is intended to serve as a conceptual piece that draws from the interplay between engineering and supply chain approaches to risk in the context of recent maritime security regulations. It is hoped that cross-disciplinary analysis of the perception and impact of the security-risk will stimulate thinking on appropriate tools and analytical frameworks for enhancing port and maritime security. In so doing, it may be possible to develop new approaches to security assessment and management, including such aspects as supply chain security.

The framework and methods reviewed in this paper could serve as a roadmap for academics, practitioners and other maritime interests to formulate risk assessment and management standards and procedures in line with the new security threats. Of particular importance, new relevant approaches can be developed to assess the reliability of the maritime in the context of the complex network theory (Bichou, 2005; Angeloudis et al., 2006; Bell et. al, 2008). Equally, further research can build on this to investigate the mechanisms and implications of security measures on port and shipping operations, including such aspects as the impacts of security on operational and supply chain efficiency (Bichou, 2008a) and the assessment of risk and return from security investments (Menachof and Risto, 2008; Bichou, 2008b).

REFERENCES

Accorsi, R, Apostolakis, G, Zio, E, 1999, Prioritising stakeholder concerns in environmental risk management, *Journal of Risk Research*, 2 (1), 11-29

Angeloudis, P, Bichou, K, M.G.H Bell and Fisk, D, Security and reliability of the liner container-shipping network: analysis of robustness using a complex network framework, In: Bichou, K, Bell, M.G.H. and Evans, A (2007), *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London

Babione, R, Kim, C.K, Rhone, E and Sanjaya, E, 2003, *Post 9/11 Security Cost Impact on Port of Seattle Import/Export Container Traffic*, University of Washington: GTTL 502 Spring Session 2003.

Bedford, T and Cooke, R, 2001, *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press

Bell, MG, Kanturska, U, Schmocker, JD, 2008, Attacker-defender models and road network vulnerability, *Philos Transact A Math Phys Eng Sci,* 366, 1893-1906

Bichou, K, Bell, M.G.H. and Evans, A, 2007a, *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London

Bichou K, Lai K.H., Lun Y.H. Venus and Cheng T.C. Edwin, 2007b, A quality management framework for liner shipping companies to implement the 24-hour advance vessel manifest rule, *Transportation Journal*, 46(1), 5-21

Bichou, K and Evans, A, 2007c, Maritime Security and Regulatory Risk-Based Models: Review and Critical Analysis. In: Bichou, K, Bell, M.G.H. and Evans, A (2007), *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London

Bichou, 2008b, 'Security Of Ships And Shipping Operations*', In Talley, 2008 (eds.), Ship Piracy and Security*, Informa, 73-88

Bichou, K and Gray, R, 2005, A critical review of conventional terminology for classifying seaports, *Transportation Research A*, 39, 75–92

Bichou, K, 2004, The ISPS code and the cost of port compliance: an initial logistics and supply chain framework for port security assessment and management, *Maritime Economics and Logistics,* 6 (4), 322-348

Bichou, K, 2005, *Maritime Security: Framework, Methods and Applications*. Report to UNCTAD, Geneva: UNCTAD, June 2005.

Bier, V.M, 1993, Statistical methods for the use of accident precursor data in estimating the frequency of rare events, *Reliability Engineering and System Safety*, 42, 267-280

Bird, F.E and Germain, G.L, 1996, Practical Loss Control Leadership, Det Norske Veritas: Alberta

Brooks, M.R and Button, K.J, 2005, Market Structures and Shipping Security, *Proceedings of the 2005 Conference of International Association of Maritime Economists*, Limasol: Cyprus, June 2005

Bureau d'Enquêtes et d'Analyse pour la Sécurité de l'Aviation Civile (BEA), 2002, *Rapport sur l'Accident de Air France Concorde F-BTSC ayant lieu le 25 Juillet 2000 à la Platte d'Oie,* Paris: Ministère de l'Equipement, du Transport et du Logement

Bureau of Transportation Statistics (BTS), 2002, Project 6 Overview: Develop Better Data on Accident Precursors or Leading Indicators, In: *Safety Numbers Conference Compendium*, Washington D.C: BTS.

Cullen, W.D, 2000, *The Ladbroke Grove Rail Inquiry*, Norwich: Her Majesty's Stationary Office

Damas, P, Supply chains at war, *American Shipper*, November 2001, 17-18

Darren, P, 2004, Smart and safe borders: the logistics of inbound cargo security, The *International Journal of Logistics Management*, (15) 2, 65-75

De Kay et al., 2002, Risk-based decision analysis in support of precautionary policies, *Journal of Risk Research*, 5 (4), 391-417

Diop, A, Hartman, D and Rexrode, D, 2007, *C-TPAT Partners Cost/Benefit Survey*, CBP: Washington DC

Erkut, E and Ingolfsson, A, 2000, Catastrophe avoidance models for hazardous materials route planning, *Transportation Science*, 43 (2), 165-179

Evers, P.T and Johnson, C.J, 2000, Performance perceptions, satisfaction, and intention: the intermodal shipper's perspective, *Transportation Journal*, 40 (2): Winter 2000

Flynn, S., 2004, *America the Vulnerable: How our Government is Failing to Protect Us from Terrorism*, NY: Harper-Collins Publishing

Fung, MK, Cheng, LK & Qiu, LD, 2003, The impact of terminal handling charges on overall shipping charges: an empirical study. *Transportation Research Part A,* 37 (8): 703-716

Gooley, T.B, 2004, C-TPAT: Separating hype from reality, *Logistics Management*, August 1, 2004

Grencser, M, Weinberg, J, Vincent D, 2003, *Port Security War Game: Implications for U.S Supply Chains*, Booz Aallen Hamilton

Guasch, J.L, 2000, *New Port Policies in Latin America and Caribbean*, New Press

Helferich, O.K and Cook, R.L, 2002, *Location and Networks: Theory and Algorithms*, MIT Press.

Hummels, J, 2001, *Time as a trade barrier*, Mimeo: Purdue University, 1-40

International Maritime Bureau On-line http://www.icc-ccs.org

International Monetary Fund (IMF), 2001, *World Economic Outlook: The Global Economy after September 11*, (http://www.imf.org/external/pubs/ft/weo/2001/03), Accessed December 2005

Menachof, D and Talas, R, 2008, The Efficient Trade Off between Security and Cost for Sea Ports: a Conceptual Model, *International Journal of Risk Assessment and Management*, Forthcoming

Joseph, G.W and Courtier, G.W, 1993, Essential management to support effective disaster planning, *International Journal of Information Management*, 13 (5), 315-325

Juttner, U, Peck, U.H and Christopher, M, 2003, Supply Chain Risk Management: Outlining an Agenda for Future Research, *International Journal of Logistics: Research and Applications*, 6 (4), 197-210

Kruk, B and Donner, M.L, 2008, *Review of Cost of Compliance with the New International Freight Transport Security Requirements*, World Bank Transport Papers, TP 16: 1-58, February 2008

Lake, E.J, Robinson, W.L and Seghetti, L.M, 2004, *Border and Transportation Security: The Complexity of the Challenge*, Washington D.C.: CRS Report RL23839

Lee, H.L and Whang, S, 2005, Higher supply chain security with lower cost: lessons from total quality management, *International Journal of Production Economics*, 96 (3), 289-300

Organisation for Economic Co-operation and Development (OECD), 2002, *The Impact of the Terrorist Attacks of 11 September 2001 on International Trading and Transport Activities*, Working Party of the Trade Committee, OECD: Paris (TD/TC/WP(2002)9/FINAL).

Organisation for Economic Co-operation and Development (OECD), 2003, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, Paris: OECD

OECD, 2004, *Report on Container Transport Security across Modes*, Report by the OECD Transport Section, Paris: OECD

Phimister, J.A, Bier, V.M, Kunreuther, H.C, 2004, *Accident Precursor Analysis and Management: Reducing Technological Risk through Diligence*, Edited book, National Academy of Engineering, Washington D.C: The National Academies Press

Rabadi, G, Pinto, C.A, Talley, W and Arnaout, J.P, 2007, 'Port recovery from security incidents: a simulation approach'. In: Bichou, K, Bell, M.G.H. and Evans, A, 2007, *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa: London, 83-94

Richardson, M, 2004, Growing vulnerability of Seaports from Terror Attacks, to protect ports while allowing global flow of trade is a new challenge, *Viewpoint,* Institute of South east Asian Studies, also available on-line at: www.iseas.edu.sg/viewpoint

Russell, D.M and Saldana J.P, 2003, Five tenets of security-aware logistics and supply chain operation, *Transportation Journal*, 42, 4, 44-54

Stavins, RN (ed.), *Economics of the Environment*, 4th Edition, Norton & Co: New York NY. pp. 378–393.

The Gore Commission, 1997, *Report to the White House on Aviation Safety and Security*, also available on-line http://www.fas.org/irp/threat/212fin~1.html

The MIT/CTS Interim Report, 2003, *Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains*. Also available on-line at: http://web.mit.edu/screspons e/repository/SC_Resp_Report_Interim_Final_8803.pdf

The U.S Federal Register, 2003, *N-RAT Assessment Exercise*, 204 (68), 60464-6046

The U.S Nuclear Regulatory Commission (US NRC), 1978, Risk *Assessment Review Group Report*, NUREG/CR- 400, NRC: Washington D.C.

The World Bank Group, 2001, *Stakeholder Analysis*, also available on-line under social development/social assessment: http://www.worldbank.org/social

Russell, D.M and Saldana J.P, 2003, Five tenets of security-aware logistics and supply chain operation, *Transportation Journal*, 42, 4, 44-54

UNCTAD, 2004, *Container Security: Major Initiatives and Related International Developments*, Report by the UNCTAD secretariat, Geneva: UNCTAD

UNCTAD, 2007, *Maritime Security: ISPS Implementation, Costs and Related Financing*, Report by the UNCTAD secretariat, Geneva: UNCTAD

Walkenhorst, P and Dihel, N, 2002, *Trade Impacts of the Terrorist Attacks of 11 September 2001: A Quantitative Assessment*, Workshop on the Economic Consequences of Global Terrorism, DIW/German Institute for Economic Research: Berlin.

Wilson, J, Mann, C, and Otsuki, T, 2003, Trade Facilitation and Economic Development: Measuring the Impact, *The World Bank Economic Review*, 17, 367-89

Willis, H.H & Ortiz, D, 2004, *Evaluating the Security of the Global Containerised Supply Chain*, RAND Technical Report series.