ENGLISH ONLY

MARITIME SECURITY: ELEMENTS OF AN ANALYTICAL FRAMEWORK FOR COMPLIANCE MEASUREMENT AND RISK ASSESSMENT

Executive summary

This document reviews the current approach to maritime transport security and suggests an alternative analytical framework that reflects better the complex nature of increasingly integrated international transport systems. The development and application of risk assessment and management techniques to maritime security must take into account the complex regulatory and operational context in which the maritime industry operates. The focus is to shift the subject of maritime security from the current agenda of facility-security to an extended framework of supply chain security.

The paper introduces an initial security risk assessment and management framework capable of reflecting the logistics scope of transport networks. The document also reviews existing approaches to measuring transport security compliance costs and funding schemes adopted by industry and governments in order to finance the costs of security regulations.

While advocating the adoption of any particular security measure is not within the scope of this analysis, the paper nevertheless argues that the new international security regulatory framework is not only a challenge, but also an opportunity to be seized. Although the new security requirements impose an additional regulatory burden on all concerned parties, security-driven business practices and operational procedures have the potential of improving efficiency and trade competitiveness.

United Nations

New York and Geneva, 2006

Table of contents

UNCTAD/SDTE/TLB/2005/4

Introduction

The adoption of the International Ship and Port Facility Security (ISPS) Code by the International Maritime Organization (IMO) and the proliferation of transport security-related measures have prompted studies aiming at reporting on relevant security-related developments, clarifying the application of the new security measures and assessing their potential impact on the international transport and trading systems.

This document is an attempt to review the current layered approach to maritime transport security and suggest alternative methods and frameworks that reflect the complex nature of increasingly integrated international transport systems. Most existing regulatory security schemes make use of a standard set of tools and various stages to assess the value and scope of potential risks and the impact of threats on the security of the maritime network. Some of these were originally developed for maritime facility security, and later applied to maritime supply chain security without making necessary adjustments.

The development and application of risk assessment and management techniques to maritime security must take into account the complex regulatory and operational context in which the maritime industry operates. The purpose here is not to propose new security-risk assessment models, but rather to point out some of the deficiencies of the existing ones in the broader perspective of the supply chain approach to maritime security.

More specifically, the paper introduces an initial security risk assessment and management framework capable of reflecting the logistics scope of transport networks. The focus is to shift the subject of maritime security from the current agenda of facility-security to an extended framework of supply chain security. The document also reviews existing approaches to measuring transport security compliance costs and funding schemes adopted by industry and governments in order to finance the costs of security regulations.

While advocating the adoption of any particular security measure is not within the scope of this analysis, the paper nevertheless not only argues that the new international security regulatory framework is a challenge, but also an opportunity to be seized. Although the new security requirements impose an additional regulatory burden on all concerned parties, security-driven business practices and operational procedures have the potential of improving efficiency and trade competitiveness.

This paper has been structured as follows: Section one provides an overview of various transport security-related initiatives including the ISPS Code; Section two addresses maritime security risk assessment and management methods and frameworks; and Section three reviews existing estimates of maritime security compliance costs and highlights the difficulties associated with collecting data on the range, distribution and magnitude of security-related implementation costs.

1. Current Transport Security Regulations and Initiatives

1.1 ISPS Code and other initiatives

In 2002 the International Maritime Organization (IMO) addressed security threats to maritime transportation systems essentially by: (a) dividing the 1974 SOLAS Chapter XI into two parts, Chapter XI-1 for Special Measures to Enhance Maritime Safety and a new Chapter XI-2 for Special Measures to Enhance Maritime Security; and (b) establishing a new International Ship and Port Facility Security (ISPS) Code to support the security regulations incorporated in the SOLAS XI-2 regulations. In addition, SOLAS XI-1 introduces the new regulation XI-1/5 requiring ships to be issued with a Continuous Synopsis Record (CSR), and modifies

regulation XI-1/3 for ships' identification numbers to be permanently visibly marked. There has been a further modification to SOLAS chapter V/19, with a new timetable for the fitting of Automated Identification Systems (AIS).

The ISPS Code itself is divided into two parts: part A is a mandatory section, while part B is a non-compulsory guidance detailing procedures to be undertaken when implementing the provisions of Part A and of SOLAS XI-2. The code sets three maritime security (MARSEC) levels ranging from low/normal (1) to high (3) in proportion to the nature/scope of the incident or the perceived security threat. MARSEC level l is compulsory and is enclosed under ISPS A. MARSEC level 2 indicates a heightened threat of security incident, while MARSEC level 3 refers to a probable or imminent threat of a security incident. Both the ISPS Code and the SOLAS amendments were adopted in December 2002 and came into force in July 2004.[1]

Other statutory instruments have been developed and implemented at various national and regional levels. The most significant initiatives are those introduced by the United States Government.[2] They include the US Maritime Transportation Security Act (MTSA) of 2002, that incorporates mandatory and voluntary ISPS provisions, the Container Security Initiative (CSI), the Customs-Trade Partnership against Terrorism (C-TPAT), and the 24-hour advance vessel manifest rule, commonly known as the "24-hour rule". Other examples include Canada's own 24-hour rule, the Secure Trade programme in the APEC Region (STAR) for Asia Pacific, the EC regulation 725/2004 extending (at two stages from 1 July 2005 and from 1 July 2007) the scope of the IMO requirements to domestic ships and associated port facilities in all existing and candidate member States, the ASEAN/Japan Maritime Transport Security Programme, and a number of IMO/ILO and WCO[3] initiatives.

Among the few industry-led initiatives, it is worth mentioning the Smart and Secure Tradelanes (SST) programme[4] as launched by the Strategic Council on Security Technology (SCST). The programme is driven by major global port operating companies and seeks to develop a technology platform to track global container movements through the incorporation a range of automatic identification technologies such as anti-intrusion sensor devices, Radio Frequency Identification (RFID) technologies and satellite (GPS, IMMARSAT) tracking systems.

---

[1] For information on IMO security regulations, see for instance http://www.imo.org/home.asp, http://www.worldshipping.org/iss_5.html, http://www.dotars.gov.au/transsec/imo/imo_isps_info.aspx.

[2] For information on US security initiatives, visit the following websites: http://www.cbp.gov, http://www.dhs.gov, http://www.marad.dot.gov, http://www.uscg.mil/hq/g-m/mp/mtsa.shtml, http://www.fda.gov/oc/bioterrorism/bioact.html, http://www.portsecuritynews.com.

[3] See for instance WCO resolution on "*The Framework of Standards to Secure and Facilitate Global Trade*" (WCO Framework) adopted in June 2005.

[4] See http://www.scst.info/. Note that the development of "secure and smart containers" is highlighted as a strategic priority under the C-TPAT programme. This implies that although the SST initiative is industry-led, a resulting container smart technology can be incorporated as an additional measure in the C-TPAT programme.

Table 1: Outline of IMO and US regulatory frameworks for maritime security

		Aim	Legal arrangements	Targets & participants	Requirements and responsibilities	Inspection & certification	Observation
IMO Package		Security of maritime network. Prevention of terrorism threats.	International mandatory rules: ISPS Code and the new SOLAS XI-2 chapter	1. Ship: 500+ GT vessels engaged in international voyage 2. Shipping company 3. Port facility, MODUs included when in port or in transit 4. Port / port operator 5. Contracting government	1/2. (1) Install SSAS & AIS. Keep security records. Display SIN. Provide security equipment. (2) Appoint SSO and CSO. Develop SSP. Undertake SSA. Keep records. Carry out training & drills. → *Obtain ISSC* 3/4. Develop and implement PFSP. Appoint PFSO. Undertake PFSA. Provide security equipment. Carry out security training & drills. Obtain statement of compliance. 5. Nominate designated authority and RSO. Approve, review and certify SSP, PFSP / PFSA. Set and notify appropriate security levels. Issue CSR. Issue & verify ISSC. Exercise compliance measures. Communicate information to IMO	1/2. ISSC issued by flag-state government or RSO (e.g. classification society) for ships and shipping companies. Maintenance of certification up to 5 years for ISSC. Interim ISSC valid for 6 months. 3/4. Validity period of PFSP/PFSA compliance statements to be decided locally by contracting government.	ISPS Part B guidelines are non-compulsory, but many countries have incorporated them on a mandatory-basis in their national security regulations.
Selected non-ISPS U.S. initiatives	**CSI**	Protect container trading systems/lanes between CSI ports and US ports.	Bilateral agreement/ partnership between the US and foreign-trade country partners.	Foreign ports (US ports under reciprocity) with substantial and direct waterborne container traffic to the US.	Establish security procedures to identify high risk container cargo. Work with deployed CBP officers to target containers at risk. Provide NII equipment for container screening & inspection.	Validation process and risk assessment mechanism (updated regularly).	CBP offers CSI reciprocity (As of April 2005, Canada & Japan customs personnel are already deployed in US ports).
	C-TPAT	Develop, maintain & implement effective security processes across the US-bound global supply chain.	Voluntary non-contractual agreement through information sharing & collaborative partnership.	Supply chain actors involved in US trade (carriers, ports, foreign manufacturers, brokers, NVOCCs, FF, etc.)	Undertake self-security assessments in accordance with CBP tailored guidelines.	Validation process to ensure consistency of participants' security practices with C-TPAT guidelines.	C-TPAT participants are offered reduced frequency screening as well as reduced risk scores in the ATS
	24-h Rule	Identify and target high-risk US-bound container cargo 24 hours in advance of loading on board a vessel destined for the US.	Compulsory rule	Ocean carriers or their agents. Licensed or registered NVOCCs.	Electronic reporting to CBP, via AMS, of complete manifest information (14 data elements) for all container exports destined for or transiting the US 24 hours prior to loading at a vessel in foreign ports.	CBP identification / clearance of transmitted information. Non- issuance or delay of permits to unload suspected cargo, or cargo with incomplete/ late advance manifest. Penalties may also apply.	Exception may be made for bulk cargo shipments. Importers/consignees may request confidentiality of their identity & the identity of their shippers. Generic descriptions (FAK, STC, general cargo) not accepted.

Acronyms and abbreviations:

AIS: Automatic Information System, AMS: Automated Manifest System, ATS: Automated targeting system, CBP: US Customs & Border Protection, CSI: Container Security Initiative, CSO: Company Security Officer, CSR: Continuous Synopsis Record, C-TPAT: Customs-Trade Partnership against Terrorism, DHS: Department of Homeland Security, FAK: Freight-all-Kind, ISSC: International Ship Security Certificate, FF: Freight Forwarders, GT: Gross Tonnage, MODUs: mobile offshore drilling units, NNI: Non-Intrusive inspectional (equipment), NVOCCs: Non-Vessel Operating Common Carriers, RSO: Recognized Security Organization, PFSA: Port Facility Security Assessment, PFSO: Port Facility Security Officer, PFSP: Port Facility Security Plan, SSO: Ship Security Officer, SIN: Ship Identification Number, SSA: Ship Security Assessment, SSAS: Ship Security Alert System, SSP: Ship Security Plan, STC: Said to Contain.

1.2 Compliance Measurement

Under the provision of the XI-2/13 SOLAS regulation, contracting governments are required to communicate specified maritime security-related information to the IMO. In an effort to compile all such information and monitor the status of compliance with SOLAS XI-2 and the ISPS Code, the organization has established the global integrated shipping information system[5] (GISIS); a database fed regularly by government communications. Up to 94 per cent of the contracting Governments to the SOLAS Convention have approved security plans for 97 per cent of the declared port facilities, while for ships a "*high degree"* of compliance has been achieved with almost "no disturbance of the world trade".[6] Note also that many non-IMO/ non-SOLAS countries have fully complied with the ISPS regulations.[7]

In Europe, a survey[8] by the European Sea Ports Organisation (ESPO) indicates that most EU port facilities are ISPS compliant at security level 1. In a port security advisory,[9] the US Coast Guard have declared seven countries as non-ISPS compliant with regard to port facility requirements and warned that vessels that have visited one of these countries during their last five port calls would be required to implement SSP security level 2 actions to enter US ports.

Regarding the US-led initiatives, the 2004 financial report[10] by the CBP indicates that C-TPAT and ISA participants account for 37 per cent of all import lines, while active CSI-ports account for 46 per cent of all entry lines for sea container traffic. These figures are due to rise given the increasing number of active CSI ports. As of 31 May 2005, CSI coverage based on listed ports by CBP accounted for 65 per cent of total US waterborne containerized imports (see table 2). A recent report[11] by the Government Accountability Office (GAO) indicates that, as of November 2004, the number of C-TPAT participants was up to 7,312 members, of which 4,153 and 409 are certified and validated respectively.

The measurement of effective compliance by type of maritime operator/actor is however very difficult to undertake on a global scale due to the variety of parties involved in the maritime transport system, but also due to different approaches of contracting State members to control and compliance measures. This may be an area of concern as to the risk of a "variant-tier pattern" of compliance control by and between contracting States[12] to the ISPS Code chapter of the SOLAS convention.

---

[5] See http://www2.imo.org/ISPSCode/ISPSInformation.aspx.

[6] IMO, 2005, *Maritime security on agenda as USCG Commandant visits IMO*, IMO Newsroom, 17 February 2005.

[7] Lloyd's List, (London) "*On the lookout of countries whose port security does not measure up"*, 15 March 2005. See SOLAS convention status at http://www.imo.org/includes/blastDataOnly.asp/data_id per cent3D11666/status.xls. See also compliance status of Taiwan Province of China (http://www.khb.gov.tw/www/service/ISPS per cent20information/ISPSINFO.pdf).

[8] ESPO, 2005, *Survey on implementation ISPS Code / EU regulation in EU ports: Status 8 months after 1 July deadline*, 8 March 2005, (http://www.espo.org.be).

[9] USCG, 2005, *Port Security Advisory: 1-05*, USGG (DHS), 28 February 2005.

[10] CBP, 2005, *Import Trade Trends: FY 2004 Year-End Report*, CBP: Washington DC, January 2005.

[11] U.S. Government Accountability Office (GAO), 2005, Cargo security: partnership programme grants importers reduced scrutiny with limited assurance of improved security, Report to Congressional Requesters, GAO-05-404, Washington DC.

[12] See for instance the different approaches to ship detention, control access, boarding procedures and certain crew-member nationals.

Table 2:

Estimated coverage of US imports by operational CSI ports (as of 31 May 2005)

Country	Port	2004 container Imports to the US (in TEUs)
Canada	Montreal	720
	Halifax	24 380
	Vancouver BC	13 590
Belgium (incl. Luxembourg)	Antwerp	304 600
	Zeebrugge	20
France	Le Havre	139 670
	Marseille	1 070
Germany	Bremen/Bremerhaven	392 180
	Hamburg	150 010
Greece	Piraeus	11 580
Italy	La Spezia	159 670
	Genoa	144 570
	Naples	29 880
	Gioia Tauro	104 480
	Livorno	92 330
Spain	Algeciras	81 750
Sweden	Gothenburg	18 810
Netherlands	Rotterdam	427 750
United Kingdom	Felixstowe	69 510
	Liverpool	39 370
	Thamesport	32 340
	Tilbury	2 560
	Southampton	38 620
Hong Kong, China	Hong Kong	1 866 320
China	Shenzhen	1 982 790
	Shanghai	1 278 500
Japan	Yokohama	109 020
	Tokyo	267 530
	Nagoya	174 940
	Kobe*	119 970
Malaysia	Port Klang	39 260
	Tanjung Pelepas	45 960
Singapore	Singapore	494 300
Republic of Korea	Busan	971 490
Thailand	Laem Chabang	201 060
United Arab Emirates	Dubai	1 110
South Africa	Durban	43 940
Total		**9 875 650**
Total 2004 US waterborne containerized import		15 805 480
Total 2004 US waterborne containerized export		8 045 045
Total 2004 US waterborne containerized trade		23 850 525
CSI coverage of US seaborne containerized imports		**62.48 per cent**

Source: Compiled and adapted from various sources including CBP, MARAD and PIERS databases.

Note: The list above includes CSI active ports only, i.e. excluding ports that have singed "in-principle" decisions but are not currently operational.

2. Risk Assessment and Security Management

2.1 General concepts

The primary aim of maritime security assessment models is to assess the level of security within and across the maritime network. When introducing the risk factor, the concept and measure of uncertainty are to be considered. Risk can loosely be defined as being the chance, in quantifiable terms, of a hazard occurrence. It therefore combines a probabilistic measure of the occurrence of an event with a measure of the consequence or impact of that event. A risk-based methodology generally consists of a five-step process: hazards identification, risk assessment, risk management with alternative options, cost-benefit analysis and decision making.

For risk identification and assessment, two main tools are generally used in engineering and safety management either the Event Tree Analysis — ETA or the Fault Tree Analysis — FTA. Both are logical diagrams: the first one focuses on events that might occur after a critical incident, while the second works the opposite way and looks at all potential incidents leading to a critical event. A typical application to maritime security in relation with the ISPS Code would be to categorize and grade scenario-risks according to their overall threat potentials using a rating scale system from 1 for minor to 3 for severe as adopted in the ISPS provisions of MARSEC levels. In both models, risks are identified, estimated, assessed and prioritized through a combination of probability and impact.

Risk management is the decision making process whereby actions are taken in view of the outcome of risk assessment. Standard risk prevention strategies aim either at reducing the probability of an incident (pre-accident intervention) or at minimising the probability of fatalities if the accident occurs (post-accident intervention). Risk management is generally combined with cost-benefit analysis (CBA) for optimal decision-making.

CBA is the most standard method for identifying the optimum benefit-to-cost ratio, usually by contrasting loss earnings, or the cost of failure, against the benefits of compliance. In the context of maritime regulation, CBA was first introduced by the Formal Safety Assessment (FSA) guidelines as approved by the IMO in 2001; and later adopted in programmes such as the ones used for regulatory assessment of maritime security (US Coast Guard, 2002; Organisation for Economic Co-operation and Development, 2003; UK Regulatory Impact Assessment, 2004).

2.2 Regulatory Risk Assessment in Maritime Security

When managing risk through legislation, regulatory assessment models are undertaken to examine the impact of policy options in terms of the costs, benefits and risks of a regulatory proposal. For the ISPS Code, examples of regulatory risk assessment models include the US National Risk Assessment Tool (N-RAT) and the UK Regulatory Impact Assessment (RIA). Those are ad-hoc exercises generally undertaken for the purpose of regulatory implementation. At the international level, the IMO/ILO framework on port-security assessment (PSA) and the 2003 OECD study on maritime security can be cited as relevant regulatory assessment exercises. In this regard, a number of observations are worth noting.

First, regulatory risk assessment are reactive by nature- that is, they are prompted and performed in relation with a proposal or a regulation already in place, and not independently.

Second, apart from initiatives such as the Smart and Secure Tradelanes (SST), there is no established *industry framework* for security-risk assessment undertaken outside the scope of government regulations and associated international mandates.

Third, available information shows that very few countries have undertaken a structured and comprehensive regulatory assessment in relation with the introduction of, for instance, the ISPS Code.

Fourth, cost-benefit analyses depicted in the existing regulatory assessment frameworks, such as the UK RIA, the OECD study, RAND reports are primarily based on methodology and techniques used to assess and compute the cost-benefit of compliance but do not consider "the resilient capacity" of the system to absorb a security incident.

Risk assessment and management tools combined with further insight gained since the coming into effect of the ISPS Code might prove useful in improving upon existing regulatory impact analyses. Cost and benefit estimates emanating from such improved regulatory assessments could contribute to an effective decision-making process.

2.3 Pitfalls in Current Risk Assessment Models

It is difficult to assess and manage risk in a uniform manner when dealing with complex-system configurations presenting low probability risks and high potential impacts, such as maritime transport. The fragmented nature of existing security risk-assessment and management frameworks results in different sets of risk assessment and risk-based decision models.

A further difficulty refers to different stakeholders' perceptions of the measure, allocation and distribution of the costs and benefits associated with a precautionary policy decision or a new regulatory programme.

Some of the problems described[13] in the context of environmental risk management may also be relevant for the purpose of security risk assessment, among them:

- Insufficient knowledge of the complex processes that determine the probability and impact of the risk.
- Combination of low subjective probability, high uncertainty, and lack of consensus.
- Rarity of the occurrence of events, and thus little actuarial or historical figures.
- Unclear pattern regarding the value, allocation, transfer and distribution of costs and benefits among both participating and non-participating parties.

In addition to the above, several problems associated with supply chain security assessment can be detected, including:

- Different approaches to the scope, nature and flow configurations of maritime supply chain linkages.
- Limited understanding of the impact of a terrorist incident on a system's supply chain disruption and resilience capabilities.
- Inadequacy of the traditional approaches (probabilistic, actuarial, historical, etc.) to modelling security-risk threats and vulnerabilities, due mainly to the lack of historical data and the irrationality of the terrorist human behaviour.
- Difficulty in quantifying and assigning costs/benefits across supply chain members with different exposure to risk.

---

[13] Page, T., 1978, A generic view of toxic chemicals and similar risks, *Ecology Law Quarterly*, 7, 204-244.

2.4 Towards a Supply Chain Risk Assessment Framework

Some central aspects of risk assessment and their meaning in the context of maritime supply chain security can be highlighted following three sources of risk:

- Environmental: uncertainties arising from external sources such as terrorist or environmental risks,
- Organizational: internal uncertainties arising within the supply chain such as strikes or production failures; and,
- Network-related: referring to the uncertainties arising from the interactions between organizations in the supply chain.

In the current maritime security regime, there is a strong emphasis on environmental and organizational risks and little focus on network-related vulnerabilities. These network-related risk sources are part of the network design and structure and their assessment is needed to avoid overlooking their capacity to absorb or amplify the impact of events from environmental or organizational risk sources.

In the context of maritime security, network-related risks include uncertainties derived from trading a non-compliant/non-certified supplier. For instance, a recent study[14] involving 20 top US firms has shown that there is a tendency among US shippers to trade off lowest bidders with known suppliers. In the context of network related security frameworks, this could imply trading-off foreign manufacturers with national suppliers; and for a global player, this could even imply trading-off producing in its own country with transferring operations abroad. The same risk-factor could also apply to trading nations, e.g. when a country's exports / imports have to be re-routed to avoid risks associated with non-compliance.

3. Compliance Costs and Funding

3.1 Estimating the Impacts of a Maritime Security Regulation

Estimating the impact of a regulation is generally performed at five different levels of analysis:

- Econometric analysis using production or cost functions to measure the impact of a regulation. The literature on the use of econometric models in the context of maritime regulation is scarce, and has usually focused on port deregulation.
- Productivity studies looking at the efficiency gains from the implementation, or absence, of a regulation. Most maritime and port efficiency studies fall under this category, yet they diverge on the definition of the concept of efficiency and the relevant data, indicators, and the methodology to be used.
- General equilibrium models aim to measure the impact of regulation on output and employment. Studies using such models have estimated the cost of regulation as varying between 7 per cent and 19 per cent of a country's GDP.[15] However, the application of general equilibrium models to maritime regulation is very sparse.

---

[14] MIT/CTS, 2003, *Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains. Interim Report of Progress and Learning*, Supply chain response to terrorism project, 08 August 2003, also available on-line at http://web.mit.edu/screspons e/repository/SC_Resp_Report_Interim_Final_8803.pdf.

[15] See Guasch, J.L. and Hahn, R.W., 1999, The costs and benefits of regulation: implications for developing countries, *The World Bank Research Observer*, 14 (1), 137-158.

- Engineering and actuarial approaches look at the added cost for equipment/procedure installation. In the maritime field, reference is usually made to premium-price analysis, whereby new costs are added to the price of port and shipping services[16]. These costs are typically assessed by analysing market response to risk-return performance, referring for instance to the variations in freight rates and insurance premiums. The latter method may prove noteworthy given the simplicity of aggregating added-insurance costs, yet it suffers from several problems including difficulties to separate rate / premium market-led variations from those prompted by security regulations and the fact that not all regulatory-driven costs are translated in insurance premiums.

- Expenditure analysis is probably the most straightforward and reliable evaluation since it relies on market surveys of additional costs as borne by the various stakeholders, both participants and indirectly affected parties. Although there is a risk of biased responses, since firms and companies tend to inflate regulatory-costs, it is possible to refine the analysis by undertaking a large scale survey and cross-examining the different responses with public market information.

  The main advantage of survey inquiries stems from their tailored approach to costs per item, facility or operator. Calculations based on cost aggregations may be challenged for the validity of the pricing systems used to calculate individual and total costs; but equally for the failure to properly consider economic and institutional structures of the various stakeholders. Elements that limit the validity of aggregate costing methods used in the context of port security under the ISPS Code, include:[17]

  - Not taking into account the cost of operational redundancies and supply chain disruptions such as ship detention and cargo delays, to supply chain disruptions such as longer lead times, higher inventory levels, and less reliable demand and supply scenarios

  - Neglecting spin-off and exponential computations of security expenses whereby market players in the shipping industry transfer costs to each others; with the ultimate user (usually shippers and cargo interests) incurring much of the aggregate cost.

  - Overlooking the world ports' organizational, operational and management systems complexities and dissimilarities. Indeed security measures targeting ports vary in time, space, scope, and nature. Indeed, physical, operational and management differences between ports, and even within a single port, constitute a serious limitation to cost compilation. PFSA, PFSP, and PFSO implementation costs will likely to vary by type and size of port facilities (berths, terminals, sheds, etc.), traffic and throughput figures, ship/cargo types, and nature/scope of landside operations (trans-shipment, storage/warehousing, intermodal arrangements, etc.).

Port-resource systems also vary considerably, and while some ports may benefit from existing facilities and resources, others will need huge initial investments and capital inputs. Port financing models should also be considered when assessing the cost of compliance, e.g. subsided versus non-subsided ports, regulatory restrictions vs. free access to private equity, type of concession agreements with private operators and users, etc.

---

[16] War risk surcharges are reported to reach between $10 to $450 per an FCL TEU, and between $5 and $12 for an LCL m^3. See for instance "War Risk Surcharge Summary", Fritz Transportation International, December 2001.

[17] 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 Economic and Logistics, 6 (4), 322-348.

There is no international benchmark rate or compensation scale for computing ISPS costs among world ports. Capital and operating costs already vary significantly between ports (e.g. differences in labour pay, interest rates, depreciation and tax systems, etc.), which makes it very difficult to construct cost-analyses on average-global approximations. In terms of scope and level of compliance, some ports choose to comply only with compulsory provisions (ISPS part A), others may consider implementing part B and other programmes. The cost of compliance will therefore vary accordingly.

A good way to analyse the cost-benefit of a regulatory change is to contrast transfer costs against efficiency costs. The first refer to the costs incurred and recovered by market players through transferring them to final customers, e.g. from ports to shipping lines to shippers. The second represent net losses in consumer/producer surpluses. Note that such analysis is not without bias, including the common practice of cost spin-off and exponential computations of security expenses.

In practice, terminal security fees as charged by ports and terminal operators vary significantly due mainly to the different approaches taken as to financing and recovery schemes. The information available at the time this report was prepared shows that container terminal security fees as charged in some major ports and terminal operators would range from no fee to US$ 19 charge per TEU. The information also indicated that import and export containers would also be differentiated, import container being applied, in such cases, a higher amount that their export counterparts. In some other cases, security charges would translate into a percentage increase of existing port dues.

Table 3: Summary of press reports on port's container security charges

Example of average terminal security fees			$/TEU
Australian ports (those operated by P&O Ports)			3.8
Europe	Belgian ports		10.98
	Denmark		61
	Dutch ports		10.37
	French ports		10.98
	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 Thamesport	19 for import and 10 for export
		Tilbury	12.7
Canada	Vancouver		2.7 per cent increase in harbour dues
	TSI Terminal handling charges		1.5
USA	Charleston, Houston and Miami		5
	Gulf seaports marine terminal conference		2
Others	Shenzhen		6.25
	Hong Kong		6.41
	Mexico		10

Source: Various news articles from *Lloyd's List, Fairplay and Containerisation International.*

Other figures suggest an average of 4 per cent initial costs and 2 per cent thereafter for maritime freight costs, between $25 to $60 levying charges per B/L, an average security charge of $6 per shipped container, and up to $40 per B/L for the 24-hour rule.[18] However, the aggregation of such figures proves extremely difficult, and a better picture would clearly require the segmentation of the market by category of trade (e.g. bulk vs. containerized trade) and participant (port, carrier, contracting government, etc.). A seaport or a contracting government need for instance to breakdown their ISPS cost structures so as to assign and examine the true incremental regulatory cost to a given market segment.

Another useful approach of particular relevance to maritime security would be to contrast the incremental costs from the ISPS regulation against the benefits from reduced maritime fraud and/or

[18] Various issues of *Lloyd's List*, *Containerisation International*, and *Fairplay*.

improved trade facilitation. A recent report by a leading consultancy firm found that the added security, including the use of security technology, would result in dramatic savings for US importers.[19] An earlier World Bank survey[20] indicates that managers in developing countries spend between 10 per cent and 30 per cent of their time managing process regulation, while another survey[21] of Latin American ports found that inefficient regulation of port operations has yielded extra tariffs on exports of up to 15 per cent. Another study concludes that each additional day in ocean transit time between two countries would reduce the probability of trade by 1 per cent (for all goods) to 1.5 per cent (for manufacturers).[22] In parallel, some estimate the cost of maritime thefts and fraud to reach a figure as high as US$ 50 billion a year.[23]

Note that the above does not include the cost of operational redundancies such as additional processing costs, ship and cargo delay, increased dwell times in ports and across the supply chain, etc.

3.2 Funding and Financing Security Regulations

Typically, there are three approaches to financing new regulations:

(a) Operators or users pay first the cost of regulation and pass it on to customers down in the supply chain, e.g. UK,

(b) Public authorities bear all the costs with no security surcharge to users, e.g. Singapore,

(c) The costs are shared between all the parties such as in terms of public grants or as a private public partnership, e.g. United States of America.

Although in most cases, a combination of two or all the above systems is used, it seems that for financing maritime security regulations different approaches have been taken on a global scale. Some countries have been funding a large amount of security costs such as through allocating grants to most ports and terminals.[24] On the other extreme, some other countries have decided to put the total burden of security financing on port operators. In this respect, it would be useful to compare port security charges as practices in the two categories of countries, and examine whether a provision for public funding is considered.

In the absence of a global tool of financing, funding should be made available on non-selective basis to ensure that compliance with maritime security measures is enforced on a level-playing field. Dulbecco and Laporte (2004) emphasize the efficiency and equity objectives of global regulation financing.[25] The objective of efficiency includes the absence of distortion on competition and that there is an incentive to contribute to the production of security. The equity objective implies that the contributive capacity of the different participant nations be taken into consideration.

---

[19] The report claims that the financial benefits for added benefits could in 80 per cent of the cases exceed $220 per container. More on this can be found in the SCST website: http://www.scst.info/releases.

[20] World Bank, 1997, *World Development Report 1997: The State in a Changing World*, NY: OUP.

[21] Guasch, J.L., 2000, New Port Policies in Latin America and Caribbean, Barcelona: New Press.

[22] Hummels, D., 2001, Time as a Trade Barrier, Purdue University, Purdue: West Lafayette, 1-40.

[23] Economic Analytical Unit 2003, *Costs of Terrorism and the Benefits of Working Together*, Department of Foreign Affairs and Trade: Canberra.

[24] For a list of security grants to ports, refer to the AAPA and the DHS websites.

[25] Dulbecco, P. and Laporte, B., 2004, Securing International Trade from Terrorism: The Financing Issue, WIDER Conference on Making Peace Work, Helsinki, June 2004, pp. 1-26.

It is worth noting that these objectives remain to be met in the context of global maritime security financing,

No single specific international mechanism or facility exists yet for financing the implementation security regulations, including for developing countries. Bilateral cooperation seems to predominate, particularly at regional levels.[26]

Additional Remarks

The lack of a comprehensive international security framework that captures the complex configurations of transport networks may be explained by the difficulty to reach a consensus between various stakeholders, including trading nations.

What seemed to be an accepted facilitating function of Government agencies has now turned into a more active role of control, monitoring and access regulation. Although prompted by well-known security threats, such a change in the perception and execution of government's role marks a breakthrough. At the same time, the mechanisms by which new security frameworks operate cannot accommodate the different components of the supply chain security system.

Notwithstanding such issues, it can be observed that in most circumstances, international trade and transport players conforming to the new security standards will benefit from being accredited for best-practice compliance. Best in class performance monitoring, cross-comparison, and competitive benchmarking could serve as a tool for gaining competitive advantage, as a successful differentiation strategy. In such a context, small and big players alike should be given the opportunity to reach the highest level of compliance with international security measures.

The issues of channel control and power, and the risk of distorting fair competition among ports need to be addressed thoroughly in both theory and practice. The same is true for regulatory and policy issues where the introduction of international initiatives based on domestic interests may lead to diverging from the multilateral approach by which the international maritime community has traditionally been structured and regulated.

A more balanced approach is needed between efficiency benefits from a deregulated environment and security requirements stemming from an increasingly regulated environment. In port security, such an approach has taken the form of cooperative arrangements between private operators and public regulators in developing, financing and implementing the various security programmes and initiatives. Such mechanisms do not, however, exist at the international maritime level and for developing countries in particular.

Finally, it is important to stress that the frameworks and methods presented in this paper are primarily illustrative. A more definitive analysis, for example, for regional or national policy issues, requires the availability of specific actual data on practical implementation and project development plans and costs.

In this regards, UNCTAD is carrying out a global survey on the implementation of the ISPS Code and a study case with selected ports that may bring some light on practical experiences. Both studies aim at obtaining a better understanding of the actual implications of the new international maritime security regime on all affected parties.

---

[26] Refer for instance bilateral cooperation between APEC countries and Australia, or between the USA and the Caribbean countries. See *Fairplay*, US may fund Caribbean security, 15 April 2004.

References, bibliography, and further readings

Bichou, K. and Gray, R., 2004, A logistics and supply chain management approach to port performance measurement, *Maritime Policy and Management*, 31 (4), 47-67

Bichou, K. and Gray, R., forthcoming, A critical review of conventional terminology for classifying seaports, *Transportation Research Part A*, 39 (1), 75-92

European Conference of Ministers of Transport, 1998, *La Desserte Terrestre des Ports Maritimes*, Round-Table 113, Paris: 10-11 December 1998

Gray, R., 2001, '*International Logistics'*, Course Materials, University of Plymouth: UK

Hesse, M., 2004, Land for logistics: locational dynamics, real estate markets and political regulation of regional distribution complexes, *Royal Dutch Geographical Journal*, 95 (2), 162-173

Holcomb, M.C., Manrodt, K.B., 2000, The shippers' perspective: transportation and logistics trends and issues, *Transportation Journal*, 40 (1), 15-25

Hoyle, B.S., 1998, 'Development dynamics at the port–city interface', In: Hoyle, B.S., Pinder, D.A., Hussain, M.S. (Eds.), *Revitalising the Waterfront. Belhaven Press*, London, pp. 3–19.

ISEMAR, 2003, *Les Transports Terrestres dans Les Futurs Pays Membres de L'Union Européenne*, Synthèse No. 55 (Mai 2003), ISEMAR: France

Lago, A., Malchow, M., and Kanafani, A., 2002, *Intermodalism and Port Competition in the United States*, Institute of Transportation Studies: University of California (also available from www.dot.gov)

Lambert, R. and Burduroglu, 2000, Measuring and Selling the Value of Logistics, *International Journal of Physical Distribution and Logistics Management*, 11 (1): 232-250

Ma, S., 1999, "*Maritime Economics"*, Lecture's Handouts, World Maritime University: Sweden

Porter, M.E., 1980, *Competitive Strategy*, New York: Macmillan Publishing, Inc.

Samuelson, P. and Nordhaus, W., 1985, *Economics*, (12th ed.), Singapore: MacGraw-Hill, Inc.

Stopford, M., 1997, *Maritime Economics*, (2nd ed.), London and New York: Routledge

Walter, C.K. and Poist, R.F., 2004, North American inland port development: international vs. domestic shipper preferences, *International Journal of Physical Distribution and Logistics Management*, 34 (7), 579-597

UNCTAD, 2003, *Manual on modernization of inland water transport for integration within a multimodal transport system*, UN: Geneva and New York