The 6th International Business research Forum:
Global Security Risks and International Competitiveness,
at
The Fox School of Business and Management
(Centre for International Business Education & Research)
Temple University, April 1-2, 2005

Assurance of Security in Maritime Supply Chains:
Conceptual Issues of vulnerability and Crisis Management

Dr Paul Barnes & Richard Oloruntoba

Abstract:

Security assurance across maritime trading systems is a critical factor for international business managers and in the evolution of international trade generally. A number of initiatives are currently underway focusing on security issues in ports and ships (International Ship & Port Security Code), customs inspections in international ports (Container Security Initiative) and whole-of-supply chain outcomes (Customs & Trade Partnership against Terrorism). The main purpose of the above initiatives is to reduce the likelihood of maritime-vectored terrorism; however inappropriate implementation of these programs could affect competitiveness.

This paper suggests that the complexity of interaction between ports, maritime operations and supply chains create vulnerabilities that require analysis that extends beyond the structured requirements of these initiatives and creates significant management challenges. Also the paper highlights the need for enhanced crisis management capabilities within ports as part of a standard management repertoire and suggests a new classification scheme for mapping vulnerability within ports and across supply networks. The paper concludes that there is a need to examine the goodness-of-fit of these security initiatives against business efficiency and competitiveness, and to consider the training needs for crisis management capabilities that will allow private and public sector groups involved in global trade to effectively mitigate the threat of maritime terrorism and loss of competitiveness.

Keywords: Maritime Security, Crisis Management, Competitiveness, Vulnerability.

1 Introduction

As the world attempted to come to terms with the events of September 11, 2001 both in regard to its impact as a major catastrophe and on international security, responses within the business world varied while impacts on businesses differed with longer-term consequences ranging from minor to extreme.

While the shutdown of domestic air space and the diversion of international flights was an obvious reaction during the initial focus of crisis management, attention moved to security in the maritime transport sector; specifically maritime trade as vector for the delivery of terrorist acts to the US mainland.

The sea-container shipping system and vulnerabilities inherent within industry practice attracted particular attention. Of concern was a capacity to covertly move contraband material, including humans, through vast and complex global supply chains. This growing concern about moving goods and services across 'economic' boundaries has arguable intensified in the years following September 11 and in the aftermath of the terrorist incidents in Bali, Madrid, Jakarta and most recently London, to the point where trading boundaries have become 'security' boundaries (Suárez de Vivero & Rodríguez Mateos, 2004).

The International Maritime Organisation (IMO), International Maritime Bureau (IMB) and other groups such as the World Customs Organisation (WCO) have jointly supported processes that enhance regulatory coverage of safety and security within the world trading system. As a result of efforts within the IMO a number of security measures have been formalised, including changes to the Safety of Life at Sea (SOLAS) Convention that specifically address ship security with updated requirements for compliance with the International Ship and Port Facility Security (ISPS) Code.

In addition to these mandatory changes, the United States has actively promoting a series of voluntary trade programmes aimed at enhancing security of trade into North American seaports and indirectly into other major trading nations. While not binding on trading partners, the measures seek to provide levels of security assurance and facilitate enhanced movement of cargo by participating ports, carriers and companies. These measures are intended to provide a competitive advantage to early voluntary adopters over time. The two principal voluntary programmes are the Container Security Initiative (CSI) and the Customs-Trade Partnership against Terrorism (C-TPAT). As recently as July 2004, 20 major trading ports had voluntarily adopted the CSI initiative (U.S. Dept. of State, 2004).

Both the CSI and C-TPAT focus on sound strategies for addressing container security, and whole-of-supply chain issues. However, these initiatives have been recognised as constituents of a framework for building a maritime security regime, and that significant gaps in security coverage will remain (Frittelli, 2003), even if adopted broadly in international settings. While such gaps in security coverage, policy and practice may be recognised there is arguably, varied appreciation of the complexity of the international trading system itself and the importance of well-integrated operational processes and security regimes within the port and host country infrastructure, and between the port and the maritime trading routes themselves.

The impact of the implementation of these voluntary initiatives on competitiveness is yet to be determined with any accuracy. This paper argues that the expected reliability and assurance of security in maritime trade will not derive from the adoption of either mandatory or voluntary trade security frameworks alone. It suggests that effective security outcomes

will result not from ensuring minimal compliance with the requirements set out in these anti-terrorist measures, but from properly integrating underlying concepts into existing managerial practice and making sure it is sustainable.

Furthermore, the reliability of such regimes will depend on how practices are incorporated into the risk and crisis management systems used by the organisations that manage port-based infrastructure and the link with other international trade-related and security assurance systems operating within the port's host country. Failure to calibrate such programmes to a fluid and changeable threat environment, as well as to the functional and business needs of exporters and importers is likely to adversely affect the effectiveness of supply chains and ultimately global competitiveness.

After detailing a number of recognised risk factors within the international maritime trading system and current security practices, this paper discusses economic impacts of terrorist activities and examines the importance of vulnerability analysis for both on and offshore aspects of maritime trade and commerce, as well as provides a useful classification scheme for types of vulnerability. The paper concludes by identifying a number of urgent issues relevant to both security policy and management practice within maritime supply chains.

2 Maritime Security Issues: Old and New

Concern by the U.S. (with growing recognition in many other countries) about shipping as a vector of terrorism is easily understood when noting that in 2001, approximately 5,400 commercial ships (most not registered in the U.S. and crewed by non-U.S. nationals) made nearly 60,000 port visits (APEC, 2003). Another view of this concern is the recognition of the complexity of modern port operations and the difficulty in effectively implementing security coverage over them (Hecker, 2002; Harrald *et. al.,* 2004).

With international maritime cargo movements at an estimated 250 million each year (circa 2003) and up to 90% of world cargo movement occurring in shipping containers, the size and complexity of this core factor staggers the imagination. Of this trade, no more than 2% undergoes physical inspection after arrival at a destination (Van de Voort, *et. al.*, 2003; OECD, 2003).

The issue of the size and complexity of modern shipping movements parallels a suite of practices that further add grounds for concern about international security issues generally. Concerns about security risk emerge from the interaction of a number of factors, namely:

- ***Cargo*** - using cargo to smuggle people and/or weapons (of a conventional, nuclear, chemical or biological nature);
- ***Vessel*** - using the vessel as a weapon or means to launch an attack (including sinking a vessel to disrupt infrastructure);
- ***People*** - using fraudulent seafarer identity to support of terrorist activities (OECD, 2003).

Another factor of concern is the lack of transparency in ship registration and ownership. A recent study on the ownership and control of ships (OECD, 2003; ICS, 1990) suggests that in addition to the absence of clarity on registration details, anonymity of ownership is a standard industry practice rather than the exception. A majority of countries tolerate 'flag-of-convenience' mechanisms. This could enable terrorists, or criminal elements, to operate or influence the use of vessels behind a cloak of anonymity. Ideally, ships like human beings must have an established identity, port of registration and nationality before setting forth on the oceans of the world. The certificate of 'Register' as the only acceptable evidence of

identity is the most important of the ship's papers, yet it is the most prone to in-transparency (ICS, 1990). Similarly, there is no conformity of qualification required for the bodies or persons who are entitled to register ships under, and claim the protection of, a particular country. Therefore the degree of control over shipowners and the conditions under which their ships trade differs in severity from flag to flag (ICS, 1990). This apply to their civic and tax liabilities, manning levels, on-board living conditions and the general maintenance of the ships themselves. On one extreme some flags require only a modest registration fee in return for a listing in the national register, while on the other extreme, the demands of the 'traditional' maritime nations include: a permanent place of business within the national territory; only nationals of the country under which the ship is to be registered appear as owners; nationals of other countries may share in ownership by investment in Limited Companies or other corporate bodies provided their place of business is in the territory where the ship is registered (ICS, 1990).

Open Registries

Years ago some countries established laws which were not compatible with traditional maritime laws the benefits of which rendered trading under these flags extremely beneficial to the shipowners to the extent that they are now a major force in world shipping. Consideration of flag is a commercial and political issue: choice of flag (registration) may decrease or increase ship operating costs. It may mean:

• paying no tax on income or;
• of preference for the carriage of freight;
• no labour restrictions and flexible wage rates;
• no fiscal control of flag authority;
• limited liability;
• no political restrictions on freedom of trade;
• no risk of nationalisation;
• minimum safety laws and regulations as well as;
• undisclosed beneficial owners are fully acceptable. In short the aim of using a 'free flags' is to circumvent trading restrictions or to operate outside national laws for political or commercial reasons. The difference today is that the use of such flags is placed firmly on a legal basis and these 'free flags' therefore serve as safe havens for shipowners (ICS, 1990).

Terrorist groups may take advantage of the current dichotomies in the international system of ship registration to make money as beneficial owners in order to finance terrorist operations, even if they do not use their ships as weapons *per se*. Panama was the first open registry to be given full international legal recognition in the 1920's, largely supported by the US government, the incentive then and now is cheap labour (ICS, 1990). Indeed in 1939 the U.S. government signed a treaty with Panama whereby profits from shipping were exempted from taxes which made it attractive to US shipowners to take advantage of freedom of employment while obtaining tax benefits. On the political front, Panama's neutrality during World War II was an additional encouragement for shipowners from the US and worldwide, to trade under the Panamanian flag (ICS, 1990). Over 100 US-controlled ships traded under the Panamanian and Honduran flags during the war and these flags of convenience proved beneficial because of the war situation. Other notable and legitimate flags of convenience are Liberia, Costa Rica and Cyprus (ICS, 1990).

Even national ship registries themselves are rarely co-located in the countries whose name they carry. Panama is considered an 'old-fashioned flag' because its consulates collect the registration fees. Langewiesche (2003) noted that a company in the U.S. state of Virginia runs 'Liberian' flagged ships, those listed in 'Cambodia' by a firm in South Korea, and the 'Bahamian' vessels by a grouping in London, England. Langewiesche (2003) comments further that while the flag-of-convenience system became regularised around World War II, it

expanded in the 1990's. By 'shopping' globally, shipowners found that they could gain commercial advantages (lower crew, operating and ship maintenance costs, and limits to the financial liabilities for loss of a ship) by choosing legal registration of their ship(s) in specific nations. Presumably, the advantages were so great those conservative and well-established shipowners, who were perhaps not naturally inclined to 'outsource' ship registration, had little choice but to conform in the face of competition.

The notion that the sea is an anarchic domain that can barely be policed even though there is a critical need to enforce relevant laws and international treaties is important. It has been noted also that the influence of the nation-state in the control of trans-national economic and business flows has weakened considerably in recent times (Suárez de Vivero & Rodríguez Mateos, 2004). This issue of variable control is particularly pertinent given the continued existence of modern and sophisticated strains of piracy and its politicised cousin, the maritime form of the new stateless terrorism (Langewiesche, 2003).

Piracy is a well-noted security issue internationally with known geographical areas of concern in the south East Asian region and other locations (Richardson, 2004a; Anonymous, 2004; Jarvis, 2003; OECD, 2003). The IMO reported 45 instances of piracy (forced boarding, cargo hi-jacking and violent assault on crews) in their reporting category the 'Far East,' in the second quarter to June 2003 (Jarvis, 2003). Over the ten-year period 1993 to 2003, 3,254 acts of piracy have been recorded in this geographical category (Jarvis, 2003). While piracy (both old and new) is an enduring factor the ISPS, the CSI and C-TPAT initiatives are new themes, at least from a policy perspective.

3 Maritime Security Programs

The requirements defined in the ISPS Code can be broken down into a number of major categories according to their focus. These are listed in Table 1 along with estimated establishment and yearly maintenance costs. The detailed requirements of the ISPS code address a number of the risk factors listed earlier.

Ship identification, security planning and alert systems have been mandated, as well as other detailed requirements for maritime carriers. The initial outlay for the ISPS is estimated to cost $1,983.8 million USD with an annual maintenance cost of $731 million (OECD, 2003).

Table 1: ISPS Code Requirements against Maritime Industry Sectors (OECD, 2003).

<table>
<tr><td colspan="2">Governments</td></tr>
<tr><td colspan="2">• Determining which port facilities are required to designate a Port Facility Security Officer.
• Ensuring completion and approval of a Port Facility Security Assessment and the Port Facility Security Plan for each port facility that serves ships engaged on international voyages.
• Approving Ship Security Plans and amendments to previously approved plans.
• Issuing International Ship Security Certificates, overseeing subsequent amendments, and exercising control and compliance measures − Communicating information to the International Maritime Organization and to the shipping and port industries</td></tr>
<tr><td colspan="2">Maritime carrier companies
Initial Cost (million USD) $1170.6 Yearly Costs (million USD) $725.6</td></tr>
<tr><td colspan="2">Companies will:
• Designate a Company Security Officer (CSO).
• Undertake a Ship Security Assessment (SSA), including an on-site visit, for every vessel to be issued a SSC.
• Develop a Flag-State-approved Ship Security Plan (SSP) that references the individual ship’s SSA and incorporates all of the elements included in part “A” of the ISPS Code.
• Designate a Ship Security Officer (SSO).
• Provide adequate training for the CSO, SSO and crew and ensuring that adequate drills and exercises are carried out.
• Ensure that vessels are equipped to carry out the security procedures outlined in their SSP’s.
• Ensure adequate security-related record keeping.</td></tr>
<tr><td colspan="2">Ships (requirements)
Initial Cost (million USD) $757.4 Yearly Costs (million USD) $4.3</td></tr>
<tr><td>Automatic Identification System</td><td>Ship-borne communication devices detailing to other AIS transponders and shore-based facilities information on the ship’s identity, position, heading and speed (Primarily designed to enhance the safety of navigation in crowded areas).</td></tr>
<tr><td>Identification number</td><td>Vessels must have a unique identification number. This number must be displayed by July 1, 2004.</td></tr>
<tr><td>Security alert system</td><td>All passenger ships, high-speed cargo vessels, chemical tankers, oil tankers and gas carriers of more than 500 gross tons must be fitted with a Ship Security Alert System that will:
• Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Flag administration, which in these circumstances may include the company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised.
• Not send the ship security alert to any other ships.
• Not raise any alarm on-board the ship.
• Continue the ship security alert until deactivated and/or reset.
• Be capable of being activated from the navigation bridge and in at least one other location.
• Conform to performance standards not inferior to those adopted by the IMO.</td></tr>
<tr><td colspan="2">Ports
Initial Cost (million USD) $55.8 Yearly Costs (million USD) $1.6</td></tr>
<tr><td colspan="2">Ports facilities that receive vessels engaged in international trade will be required to:
• Carry out, and have approved, port facility security assessments.
• Develop port facility security plans that detail measures to be taken at each security alert level, and address single-ship security alerts.
• Designate a Port Facility Security Officer (PFSO) with skills and training roughly similar to the CSO.
• Ensure that the PFSO and other appropriate personnel receive adequate training to carry out their duties and that security drills are held to ensure the readiness.
• Ensure that port facilities are sufficiently equipped and staffed in order to operate under relevant security levels and meet certification/documentary requirements.</td></tr>
</table>

The CSI programme however is a unilateral effort that seeks to develop bi-lateral agreements between the United States and foreign countries with significant container trade volumes into the U.S. A general aim is to pre-screen high-risk containers in ports of loading. While the majority of container movements pose little or no security threat, all identified high-risk containers will be inspected either before loading at a CSI port or, if arriving from a non-participant port upon arrival in the United States. In CSI active ports, local customs officials and U.S. Bureau of Customs and Border Protection staff would jointly decide on which containers to inspect before loading. The initiative is built around four principal elements shown below:

- Establish security criteria to identify high-risk containers.
- Pre-screen those containers prior to arrival at US ports.
- (Involves the deployment of American Customs officials to foreign ports) Use technological means to pre-screen these containers.
- Develop and use IT-enabled and secure containers (OECD, 2003).

The C-TPAT initiative has much broader aims that seek to ensure that participants implement policies, plans and procedures to ensure the integrity of their entire supply chain. Participants will be expected to sign agreements committing to the actions listed below:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by U.S. Customs and the trade community covering: Procedural Security, Physical Security, Personnel Security, Education and Training, Access Controls, Manifest Procedures, and Conveyance Security (Participants must also submit a supply chain security profile to U.S. Customs).
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines.
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies (OECD, 2003).

The expected costs to participants from voluntary compliance include investment in securing the physical integrity of their own premises and that of their trading partners as well. Other costs include personnel training, adding security guards, developing security risk management plans and processing C-TPAT system requirements. It is likely that involvement in the C-TPAT initiative will require substantial investment for many industry sectors even though many already have effective security practices in place to reduce theft (OECD, 2003). Beyond issues of costs it is likely that full implementation of the C-TPAT system, because of its intrusive scope, would require detailed negotiations among companies and national authorities engaged in international trade at all trading countries.

4 The Economic Impacts of Maritime Threats

Maritime security threats and the plethora of other active threat sources introduce high levels of uncertainty to business considerations and the world economy generally. Any disruption of maritime supply has significant implications on economic activity and world trade. It has been suggested that investment in the United States dropped by 0.2 per cent of GDP because of the ongoing threat of terrorism (Saxton, 2002).

In addition, the generic effects of concern about future terrorist incidents have adversely affected many developed and developing economies. Certain economies within the Asia-Pacific Economic Cooperation (APEC) region for example, were also affected with decreased Foreign Direct Investment (FDI) and influenced by existing vulnerabilities due to reliance on

maritime trade and the presence of on-going instances of piracy (Commonwealth of Australia, 2003; OECD, 2003).

International trade is heavily reliant on safe and open waterways and oceans. A significant downstream consequence of a terrorist attack on the maritime transport system would most definitely entail disruption of supply resulting in a range of impacts. For example, a major security incident such as a suicide attack using a vessel on an oil platform would not only disrupt the supply of oil and gas and other natural resources but also pollute the sea (Regional Maritime Security Initiative, 2004). In addition, the loss of vessels, cargo and crew lives coupled with the diversion of productive resources to security measures, would negatively affect economic activities.

A range of economic costs resulting from terrorism generally and other disruptions to business continuity has been estimated and documented in broad economic terms. A study of covering 200 countries from 1968 to 1979 found a doubling of the number of terrorist incidents and decreased bilateral trade between targeted economies of some 6 percent (Nitsch & Schumacher, 2002). According to *Fortune* magazine of 18 February, 2002 the impact on US supply chains due to increased inventories, border closures, increased lead times and other changes and security measures resulting from the events of September 11, 2001 is estimated at USD 150 billion a year. Such incidents will negatively affect travel time and transport costs as destroyed infrastructure is rebuilt (Kwek and Goswami, 2004; Thissen, 2004).

Gooley and Cooke (2002) reported the consequences of a two-week industrial dispute at 29 US West Coast ports in late 2002. More than 200 ships (carrying 300,000 containers) remained unloaded while rail and other inter-modal shipments were delayed across large sections of the transport network. As a result export cargoes filled warehouses; cold storage and grain silos on both sides of the Pacific Ocean, while costly mid-ocean diversions of maritime traffic to other ports ensued and businesses laid-off workers or cut back production. Estimates of losses from this disruption to US West coast ports in 2002 indicate a 0.4 per cent reduction of nominal GDP in a number of Asian economies. The impact on Hong Kong, Malaysia and Singapore in particular was estimated to be as high as 1.1 per cent of nominal GDP (Saywell & Borsuk 2002).

The September 11 attacks against the World Trade Centre (WTC) led to $19 USD Billion in insured property losses and an estimated economic loss of up to $90 USD Billion in 2001 terms (Schaad, 2002). The immediate costs of terrorism include loss of lives, destruction of property and depression of short-term economic activity. These costs are further compounded by the uncertainty associated with the continuing threat of terrorism as productive resources are diverted to preventive security measures (Raby, 2003).

Another category of short-term cost relates to the effects of increased uncertainty on investment and consumer behaviour. Uncertainty was immediately transmitted to the financial markets while a sharp upward re-pricing of financial risk exposure occurred. Increased uncertainty boosted market volatility thereby increasing risk premiums. Consequently, insurance costs are a critical issue as rising premiums add to the costs of doing business. A sea-borne terrorist incident whether using conventional or improvised explosive devices or involving chemical, biological, or nuclear materials would impact heavily on the availability and cost of marine insurance as would a major act of piracy. Premiums were tripled for ships calling at ports in Yemen after the 2002 terrorist attack on the French oil tanker *Limburg* off the Yemeni coast. This forced many vessels to cancel Yemen from their schedules or divert to ports in neighbouring states (Richardson, 2004b).

In addition to increased insurance and re-insurance costs a catastrophic sea-borne terrorist attack would cause delays in shipping or at best, increase transit times for commodity movements. Such disruptions of the supply chain would have repercussions around the world and profoundly affect business confidence (Richardson, 2004b). In addition, increased uncertainty has a negative depressing impact on consumption as business confidence deteriorates. These negative effects impacted some industrial sectors more significantly than others after September 11 for example; abnormal losses were documented in the airlines sector, as well as the travel, tourism, aerospace, hotel, restaurant and gambling industries (Saxton, 2002).

Permanently increased security coverage with enhanced vigilance at air and maritime ports is expensive. Additional security checks and inspections, including information requirements contribute to delays at air and border posts. In addition, the long-term capital investment in new or upgraded infrastructure and organisational restructuring within governments add to the burden of doing business and maintaining competitiveness generally (Saxton, 2002).

5 Maritime Supply Chains and Global Competitiveness

Effective and efficient systems of transportation are critical to domestic and international business. Along with trade liberalisation, the adoption of international standards, advanced telecommunications and the capacity to transport goods and commodities are critical factors in globalised and interdependent economies (Kumar & Hoffman, 2002). In addition, effective and efficient systems of transportation are critical to optimising transport and transaction costs and global competitiveness generally.

A study by the World Bank found that increased port efficiency has a significant and positive impact on the expansion of trade, as are improvements in the customs regulatory environment. Therefore it can be deduced that burdensome customs and regulatory/security measures may hinder port efficiency and the efficiency of maritime supply chains which in turn leads to a contraction in trade and overall efficiency (Wilson, Mann & Otsuki, 2003).

While the notion of a competitive company is clear, the notion of a competitive nation is not. Ultimately, the source of competitive advantage rests at the industry level and regional level. Studies have been conducted to examine firms and industries in order to determine what confers advantage to particular industry sectors and the policy positions that governments might pursue to generate a competitive edge for domestic industries (Garelli, 2001; Farrugia, 2002).

The International Institute for Management Development considers aspects of structural factors affecting long term economic performance as encapsulated in the concept of competitiveness with respect to productivity, skills and innovation in the economy (Fagerberg, 1996). Not-with-standing notions of global competitiveness, the focus of this article is on regional competitiveness. This makes considerable sense in that any loss of competitiveness in trade will impact directly on regional economies especially those with a higher than average density of trade-related infrastructure that would normally be found within ports and their hinterlands.

An Economic Impact study carried out by the St Lawrence Seaway Development Corporation (SLSDC) in 2001 highlights how the presence of an efficient maritime trading system can enhance regional competitiveness. The study included the St. Lawrence Seaway and related waterways, ports and their inter-modal connections, as well as vessels, vehicles and other system users. The SLSDC report indicated a total of 152,508 jobs are in some way related to

the 192 million tonnes of cargo moving on the US side of the great lakes seaway system in 2000 (U.S. Dept of Transportation, 2002).

In addition firms providing transportation services and cargo handling services made USD$ 1.3 billion of purchases in the great lakes region that supported 26,757 *indirect j*obs. Maritime activity on the U.S. side of the great lakes seaway system generated USD$ 3.4 billion of business revenues for firms providing transportation and cargo handling services. This excludes the value of the commodities moved on the great lakes seaway system. Maritime activity on the U.S. side of the great lakes seaway system created USD$ 1.3 billion in federal, state and local tax revenue in 2000. Firms providing the cargo handling and transportation services spent USD$ 1.3 billion on purchases for a range of service-related deliverables: for example diesel fuel, utilities, maintenance and repair services (U.S. Dept of Transportation, 2002).

Thus, the perturbation of an effective supply chain 'moving' through a large hub-port would have a significant impact on competitiveness in nearby regions with expected losses to local and regional economies. One of the key factors that would reduce competitiveness is vulnerability within the management structures or specific sub-section of a port, the in-country interface and adjoining hinterland, and more broadly, elements of the supply chain(s) as discussed in the following section.

5 Vulnerability - On and Off-shore

Ports have become pieces of critical infrastructure within trading systems especially in relation to economic performance at the national and international level. Certain key locations have been classified as 'hub Ports' which, due to their size and capacity have become essential to the efficient functioning of the global supply network (Bateman, 2003). The consequence of shutdowns in ports on the U.S. west coast on Pacific Ocean trade operations was noted earlier in the paper. In such circumstances, vessels can usually re-route around a chokepoint, with added costs in terms of time efficiencies. Nevertheless, the threat of loss of a substantial port facility is a major critical infrastructure protection issue. A further element requiring protection at a port is the automated control systems used in many modern hub-ports including, in particular, embedded information technology and information systems such as Vessel Traffic Systems (VTS) as well as other ubiquitous information and communications technology (ICT) infrastructure.

A security incident (or multiple concurrent incidents) may occur at any time in large highly complex systems such as a supply chain or trading network. Incidents might occur in a number of ways: by emerging suddenly due to the interaction of previously separated system elements, or by 'cooking' slowly without recognition until they appear. In either case, the incidents are often surprising, unexpected or both. The literature on complex systems failure suggests that in many cases on investigation, evidence was discovered that there had been 'signs' that crisis was emerging from organisational 'noise' (Perrow, 1984; Turner & Pidgeon 1997; Boin & Lagadec, 2000; Comfort *et. al.*, 2001, Rijpma, 1997).

The 'incubation' of these failures over time and the failure to note the presence of 'warning signs' are symptoms of organisations that have been termed 'crisis prone' (Turner & Pidgeon 1997; Pearson & Mitroff, 1993; Mitroff & Alpaslan, 2003). In addition to failing to notice the evident signs organizations can lack the functional systems to respond to them. Equally there are situations where, as a result of extreme systems complexity warning signs may not have been visible or if detectable, not understood. While not in the same category as the 'ideal' situation above where a crisis 'signals' it's impending arrival and may have been detected,

this second category may be the result of a totally new systems behaviour or some other source of perturbation.

6 Systems Complexity, Crisis and Vulnerability

Crisis management theorists have emphasised the need for business managers to extend their conceptual frames from models of the *world as a simple machine* to the *world as a complex system* (Mitroff & Kilmann, 1984). In this sense, circumstances under which expected organisational functioning 'transitions' from normality to crisis may be an analogue of moving from regularity (familiar - expected functioning) to the edge of chaos (unmanageable complexity).

Maritime supply chains are susceptible to terrorism and other perturbations because of their open nature nationally and globally, and their complexity (Van de Voort *et. al.*, 2003). In addition, the complex organisation coupled with the unique vulnerabilities of ports and associated support components are not easily appreciated or understood (Harrald, Stephens & van Dorp, 2004). Indeed, the U.S. Government Accounting Office has similarly suggested that difficulties in coordination amongst public and private entities active at the port itself and with an interest in port security may make effective security programs hard to establish (Hecker, 2002).

For explanatory and conceptual purposes, the notion of interactive complexity is critical to maritime security in the sense that the potential for incidents or inefficiencies exist because of vulnerabilities inherent in the design and operation of ports, and in their interaction with maritime supply chains. Vulnerability is defined in this paper as a susceptibility to change or loss because of existing organisational or functional practices or conditions. In examining these factors, this paper defines two distinct classifications of vulnerability: namely Type 1 and Type 2.

Type 1 Vulnerability emerges from the operational complexity within a port encompassing the transport node infrastructure and onsite operators. As previously noted, processes at ports and in related systems, can be difficult to coordinate. Harrald, Stephens and van Dorp (2004) describe Ports as "critical nodes in complex economic inter-modal subsystems that facilitate the movement of goods and cargo around the world." Cargo and passengers are transferred to and from the maritime mode connecting them with other transportation modes (e.g. rail, road, or pipeline). Although individual modes (as stand alone systems) may be tightly connected, the functional links to other systems within a port can be relatively loose. A container facility is for example, 'tightly coupled' with the inter-modal rail yard and the tightly scheduled container vessels, but only loosely connected with the adjacent petroleum facility or cruise terminal.

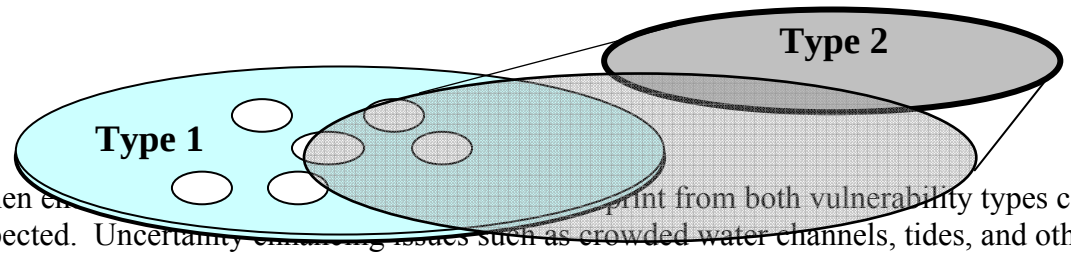
Before the mandated ISPS requirements were implemented internationally, comprehensive security[1] outcomes may not have been a core design criterion for many of these maritime sub-systems, other than basic provisions for preventing criminal theft and violence. This absence of in-built security in the segregated sub-systems means the retrofitting of security at international ports will be more than just enhanced asset protection. A port security framework logically, would need to extend well ashore, for example security for containers and other general trade movements, as well as passenger vessels. Currently, vulnerabilities inherent in such complex economic systems (ports) are not adequately understood (Harrald, Stephens and van Dorp, 2004).

[1] It is assumed that bio-security requirements have been critical aspects of existing port procedures however.

This form of vulnerability might be contributed to by 'loose' organisation and coordination mechanisms including risk management and/or corporate governance resulting in a reduced capacity to detect warning signs or understand their meaning. This reduced capacity might also be contributed to by inflexible cultural factors or belief systems within an organisation itself that promotes notions of invulnerability or indifference to external or internal threats (Boin & Lagadec, 2000). Group think (Janis, 1982) as a cultural factor at the organisational level can also be a manifestation of this phenomenon. As such, *Type 1* Vulnerability could be diagnosed as an emergent tendency of the organizations within a port precinct to generate moderate to higher frequency - low consequence incidents.

The *Type 2* Vulnerability is an attribute of maritime movements, with ports as nodes of the system and global logistics management practices underpinning the supply chains. Together they form a 'system of systems' exhibiting considerable uncertainty as well as intense and fragile interactive complexity.[2] On the high seas, the system components include the ship (and other ships depending on sea lane traffic), radio and networked communication, the weather, the cargoes being transported and orders from ship owners (Perrow, 1984). Figure 1 represents an illustration of this system-of-systems.

Figure 1: Convergence of Type 1 and 2 Vulnerability



When el[illegible]print from both vulnerability types could be expected. Uncertainty emanating issues such as crowded water channels, tides, and other geo-physical effects, pilotage, navigation controls (including back ground light from the shore) and the speed of loading and discharge are operational aspects of the converging systems requiring control (Perrow, 1984). The frequency of ship movements along major trade routes, as well as within congested coastal waters can be high, especially for hub ports. While efficiency may be an expected factor in stevedoring operations and the operation of port-based transportation infrastructure, once a ship departs port reliance on such regularity, certainty and control cannot be assured.

The vagaries of the 'high-seas,' manifesting as storm and tempest alone remain important uncertainties even in the current age of satellite communications and geographical positioning systems. Modern forms of piracy and trans-national criminality add further complexity to this equation. An important factor to be considered is the overlap of system boundaries between the Maritime and Port regimes and how crisis and security management issues can be dealt with across this divide.

Just-in-time manufacturing, quick response, single sourcing and reduced inventory strategies are examples of common approaches to logistics and supply chain management. They work more effectively however in times of market stability but less so in times when the volatility of demand increases (The Home Office, 2002). The nature of doing business in this modern form itself generates vulnerability due to the mutual interdependencies of stakeholders within the supply networks. The fragility of these interdependencies creates reduced resilience in the wider systems and can lead to unexpected or surprising juxtapositioning of causal elements,

[2] Interactive complexity as used here relates to unfamiliar, unplanned or unique operational sequences that might not be visible or comprehensible to users of the system and could cause or contribute to errors or loss events (See Perrow, 1984).

thus resulting in system failure. Within maritime trading systems, a form of 'normal accident'[3] (Perrow, 1984) might be expected but not necessarily predictable.

A coordinated security regime targeting world trade[4] would have to operate under the dual constraints of the presence of both Type 1 vulnerability: emerging from the interactive sub-systems of a port and the port and in-country interface, and Type 2 vulnerability: system of systems factors combining logistics industry practice and marine movements. Conceptually, a maritime supply chain may be expected to exhibit a tendency towards both sources of vulnerability albeit with regional and geographical variation.

7 Issues for Policy and Practice

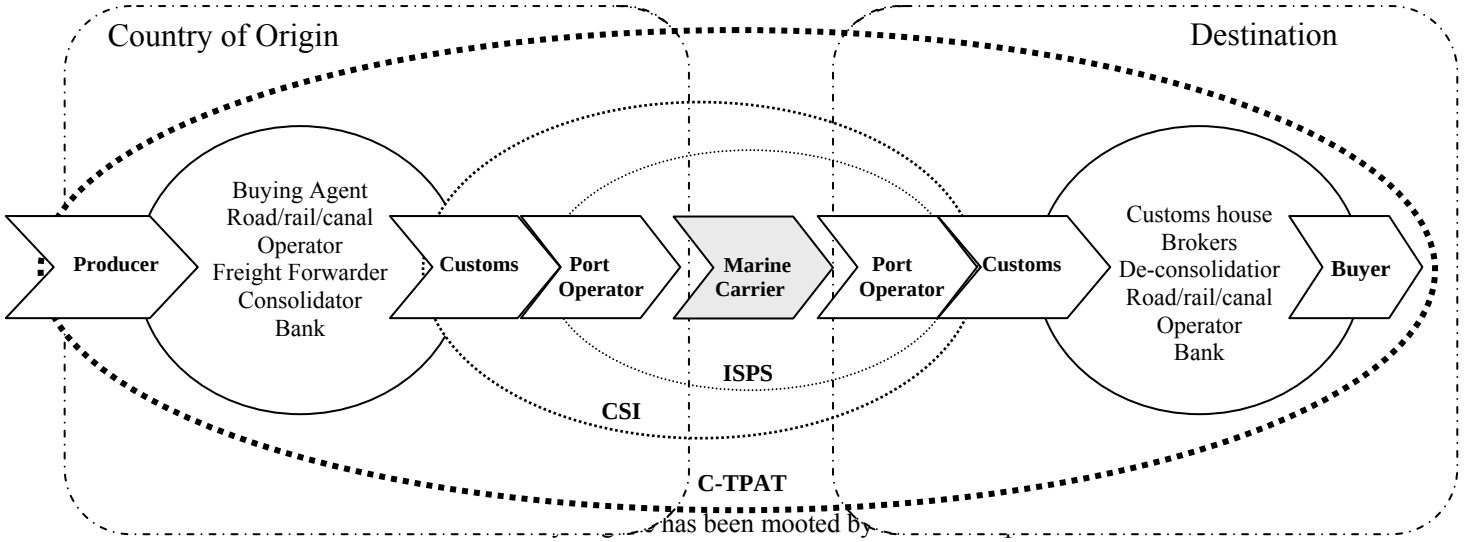
The intricacies of global supply chains have increased, and a proactive identification of relevant trans-national vulnerabilities by governments and corporations is required as is the input of this knowledge into trade policy debates at the highest level.

The scope of all three maritime security initiatives is shown in Figure 1. The C-TPAT framework is arguably, a partial extension of the CSI with much detail in coverage encompassing both commercial participants in trading countries of origin and destination. Logically, if extended to its extreme, the C-TPAT initiative would affect industrial production lifecycles and wholesale/retail links in addition to supply chain effectiveness and efficiency. A number of these critical issues are likely to impinge on the way international business is carried out and need to be investigated in much detail.

For example, on aggregate the multi and unilateral security regimes requiring oversight will influence the choice of optimising strategies for many global logistics and global procurement providers. They would also influence options for stockpiling of supplies (with related inventory inefficiencies) internationally with a particular focus on counties of origin and destination. At present the ISPS, CSI and C-TPAT programmes are focused on reducing the likelihood of terrorist related incidents within program areas and not to strike a balance between efficiencies within the supply chain networks and requisite security assurances.

This issue requires debate and close examination within trading and international business circles given the collaborative intricacies inherent in the descriptive elements of the supply chain shown below.

Figure 2: Scope of IMO and US Maritime Security Initiatives across a Supply Chain
(OECD 2003)



has been mooted by

Given the potential impacts on business in terms of compliance costs related to these initiatives it may be logical to assume that appropriate economic (competitiveness) impact analyses had been examined within and across major trading blocs before the measures were unilaterally applied, however there is no evidence to support this assumption as governments often impose initiatives on business without considering the financial impact. Nevertheless, failure to examine the impact(s) on operational businesses processes and competitiveness would achieve little, as the added cost of doing business would act a disincentive to many companies, especially given the scope and intricacy of the C-TPAT Initiative.

A myriad of participants exist in any pre-customs (origin) and post-customs (destination) elements of a maritime supply chain. From Figure 2 the complexity purely from a transaction perspective is noteworthy. Interactions include buying agents, road/rail transport operators, freight forwarders and consolidators – all having some degree of contact with commodities being shipped. At the destination similar participants engage in dispersal of goods.

In addition to the added burden of regulatory compliance with CSI and/or C-TPAT business operators within a port are likely to have to maintain effective relations with police and emergency services, customs, quarantine and port health officials, their clients and their own suppliers. Transactions within and external to this network would be complex during normal operations. How these functions would be managed during the transition to a crisis requires some thought. As mentioned previously, crises generically emerge in two forms: the 'slow cooking' (or incubator), and the 'fast mover.' How the country of origin or destination stakeholders would interact during either variation of crisis type is important.

As a thought experiment, consider what in Australia has been a real maritime trade practice: the live export of cattle to the Middle East. How would operators within a maritime supply chain respond to the threat of contamination of stock or 'reports' that certain cattle had displayed symptoms of a notifiable economic disease while in feedlots awaiting shipment? One particular strategic viewpoint might be to think of the situation as a large product tampering issue. However, given the recent ban on the importation of U.S. beef into Japan, the epidemic of Foot-and-Mouth Disease and Bovine Spongiform Encephalopathy in the U.K. and concerns about bio-security generally, such a view would be totally inadequate and wrong. Such an event would require scalable capacities for crisis response that are embedded within the operational repertoire of port management and onsite operators.

As an extension of our thought experiment, consider further the likely response to the detection of bio-contaminants or fugitive gases in a container that tested positive for a 'signature' of materials known to be precursors in the preparation of weapons-of-mass-destruction. The normal functions of all port-based participants would be disrupted by a very rapid response from government security and response agencies. In addition to disruption of ship movements into and out of the port, state, federal and international security interest would focus rapidly on the situation.

In such circumstances, the intense scrutiny from regulators and the media would reveal any failure on the part of authorities in charge of the port to have examined crisis planning contingencies for on and offsite stakeholders. If the situation had been foreseeable, the

absence of suitable consideration for crisis management could cause a degree of embarrassment.

This paper seeks to emphasise three factors in the broader analysis of supply chain security and in particular issues for policy and practice. These are: recognition of the emergence of crisis; development of crisis management capabilities; and miscellaneous practical management strategies for firms involved in trade and port operations. These are considered below.

Crisis Recognition:
The absence of a crisis management capability within organisations has been noted extensively in the literature covering industrial disasters and business and organisational failure as a major weakness.[5] As mentioned earlier both 'slow' and 'rapid' onset crises emerge readily in highly complex systems. The existence of both internal (Type 1) and external (Type 2) vulnerability within maritime trading systems increases the vigilance needed within all globalised organizations. Crises often create situations that cannot be anticipated, so 'warning sign' detection is critical as is a tested ability to respond to emergencies quickly and effectively (Boin & Lagadec, 2000). The need to have a trained and responsive crisis management team seems obvious.

The degree of forewarning available to management is often dependent on the sophistication of existing organisational monitoring systems available. A crisis management capability of this nature would entail a robust threat assessment capacity that includes sub-functions for:

- *Environmental Scanning* (warning signs);
- *Emergency Management Escalation Triggers* (incident/issue recognition);
- *Consequence Analysis* (understanding how multiple cascading impacts can occur and where they will manifest);
- *Crisis Coordination and Decision-making Capacity* (separate to routine business decision making structures) (Barnes, 2001).

An additional capability is a clearly stated, understood and tested communication mechanism for reporting emergent incident/issues to senior decision makers.

The benefits of such capacities have been recognized within specific industries internationally but how they might be established at the level needed for consistency across the maritime trading industry is yet to be determined. The degree to which crisis management skills would assist the delivery of security assurance and risk management outcomes within wider international business settings also warrants serious examination. With some notable exceptions,[6] such investigations have historically been absent from mainstream international business literature.

This absence might be explained by the rate of knowledge diffusion of what is ostensibly a paradigm shift in the analysis of organizational failure. This change is centred on recognition and analysis of complexity within organisations and business, and the importance of cultural factors that increase vulnerability and thus susceptibility to crises. This 'shift' allows a more comprehensive understanding of crisis and risk management as it can be applied to complex human activity systems.

[5] See for example: Turner & Pidgeon 1997; Pearson & Mitroff, 1993; Mitroff & Alpaslan, 2003.
[6] See Shaw & Harrald (2004).

A well-established theme within this emergent body of organisational failure research – the System Accident – deals with the notions of interactive complexity (Perrow, 1984). When the system is interactively complex, inter-dependent failure events can interact in ways that might not be predictable by the designers and operators of the system. The effect of such failures can spiral out of control before operators are able to understand the situation and perform appropriate corrective actions. In such systems, apparently trivial incidents might cause cascading impacts that interact in unpredictable ways with possibly severe consequences (Marais *et. al.*, 2004). This research theme is the genesis of the concept of Type 1 vulnerability.

An additional explanation for the absence of coherent work in this area is that complexity theory, as a conceptual and analytical tool within commerce, organisational design and functional management is becoming a paramount theme in effective corporate and operational management in the public and private sectors globally (Mahon and Cochran, 1991). More recently, Robertson (2004) has supported this contention in discussing organisations from the perspective of complex adaptive systems. While the application of these concepts seems both interesting and logical, their successful use will not be simple. A further consideration is that many researchers and managers may not fully appreciate the critical linkages between organisational competitiveness and the capacity to respond quickly to, and recover from crisis events as embodied in business continuity planning.

Development of Crisis Management Skill-sets:
How might a Crisis Management capability be developed? A first step is to ensure the support of senior management and especially the CEO for the processes involved and the benefits that can accrue. A second point is the recognition that a crisis management capacity can be grown or at least bootstrapped to existing occupational health and safety and security structures. The following needs should also be considered:

- The creation of new skills in applying foresight (via interdisciplinary teams) to issues that can limit achievement of organisational and business goals;
- Ensuring that robust analytical and conceptual frameworks of security risk management and corporate governance are developed appropriate to the functions and purpose of the business (Barnes, 2001).

The costs or barriers associated with developing sound crisis management skills include financial outlays (initial and sustaining), training and the potential for 'losing' experienced and skilled staff to competitors or other industries. The effective management of crisis within organisations require the application of different sets of skills often not normally used in the day-to-day running of a business. A simple explanation as to why such skill-sets are not yet widespread in maritime and other industries is that their need may have not become readily obvious and easily justified as directly contributing to profits or the bottom-line.

This position is questionable however, because according to conventional economics, reduction in costs associated with disruptions to business continuity such as a preventable crisis, terrorist attack or public relations blunders will translate to lower cost profiles, and a positive corporate reputation in the mind of the customers, public and business partners.

A further explanation is that conceptually *risk* is sometimes narrowly defined and limited in scope within business settings with a focus on: loss and prevention control; insurance coverage; or information security; and financial and audit control functions. Higher order strategies such as contingency and business continuity planning which encompass a

sophisticated implementation of risk management may be seen as unaffordable in terms of time, people and money.

Thus, crisis management too as a higher-order business repertoire is effectively shorthand for management practices subsumed into institutional and organisational responses to non-routine events. Rhinard, Ekengren, and Boin (2004) suggest that specific challenges can be categorised under four headings: *Prevention* - recognition systems for emerging crises; *Preparation* - planning for the unknown; *Response* - making effective decisions and having them implemented; and *Recovery* - restoring normality and learning. However, both *preventing* and *preparing* for crisis-situations presumes a deep and effective understanding of the way in which the 'unknown' factors and conditions can manifest.

This level of understanding presumes a means by which people can make sense of confusing circumstances. Equally important is the capacity to effectively generate an organisational response in crises. This can be difficult because due to differences between international judicial and regulatory systems, the cascading effects of crises can manifest over varying time scales with different primary, secondary and tertiary consequences. Management skills such as the ability to analyse security and political risk or the ability to gather information and business intelligence as well as the ability to bring effective leadership and decision making abilities to bear during crisis situations enhances the reduction of organisational losses and confusion during crises.

Miscellaneous management strategies

The crisis management capacities discussed above should not be construed as stand-alone solutions. Other corporate strategies are beneficial and will logically include ensuring transparency and trust amongst corporate stakeholders within supply chains, members of trade blocs and especially governments and government regulators. This can be supported through large-scale education of all stakeholders to the dangers of information hoarding, complacency and 'group think'. Partnerships may also be developed across the various stakeholders.

In a practical sense, maritime security issues are strongly linked to international law and especially the conventions on Maritime law. Within the South East Asian and Oceania region, members of the maritime trading industry are supporting reinforcement of detailed foreign policy action by a number of nations. Particular support is being provided for ongoing processes of international consultation and cooperation on preventing terrorism including maritime piracy. These processes are pursued under the auspices of the Asia Pacific Economic Cooperation (APEC) and the Association of South East Asian Nations (ASEAN).

The Secure Trade in the APEC Region (STAR) Initiative for example, seeks to strengthen maritime security against terrorism while boosting trade efficiency. In addition to supporting the implementation of the ISPS Code, this initiative encourages implementation of harmonized standards across a number of critical security areas. These include electronic customs reporting (a World Customs Organisation program), comprehensive baggage screening procedures and mandatory aviation security audits required by the International Civil Aviation Organisation, and the implementation of a common standard for the collection and transmission of advanced passenger information to prevent the fraudulent use of travel documents by terrorists APEC (2003). The STAR Initiative seeks to generate new partnerships between government and business at the national and international level resulting in mitigation of terrorist or criminal threats throughout the supply and logistics chain. In addition to the obvious goals of protecting cargo, ships, people and in combating threats to security, key goals of the initiative include harmonizing trade and anti-terrorist legislation,

cargo screening technologies and importantly, sharing supply chain and data and intelligence (APEC, 2005).

Another example of efforts by industry participants involves participation in the recent ASEAN Regional Forum (ARF) activity as it moves from traditional attention to inter-state power relations towards commonly perceived threats such as international terrorism, piracy at sea, arms smuggling and other trans-national crime. Greater cooperation has been pledged by ARF members on these areas of concern, in particular threats to maritime security (Severin, 2003). Dialogue on these broader issues including trans-national crime is also being developed through the activities of the Council for Security Cooperation in the Asia Pacific (CSCAP, 2003).

8 Suggestions for further Research and Inquiry

While concern about security at U.S. ports existed before September 11 (Fritelli, 2003), the extent of the complete threat environment including fragility of supply chain continuity and the interactive vulnerability of port and trade routes remain unappreciated. The interactive complexity of the 'system of systems,' as it manifests across the two vulnerability regimes require careful and comprehensive analysis to uncover corporate exposures and detail mitigation options for management. It is recognised that other emergent phenomena such as climate change, public and animal health crises and the increasing hyper-complexity of embedded information-communications-technology (ICT) also affect global and regional trade and business practices. Failure or instability arising from any of these sources can trigger cascading impacts, often through unexpected pathways and fault lines and throughout the wider supply networks and trading systems.

Because of these cascading phenomena, institutions within maritime trades would be unlikely to face single incidents but rather systemic failures appearing concurrently. Lagadec & Michel-Kerjan (2004) refer to such a tendency to ubiquitousness as a 'Network Factor. Unexpected convergence of factors affecting human-systems can generate effect propagation via connectedness and interoperability of these same systems. Crises such as these have been described as 'outside of the box,' too fast, too strange and too costly (Lagadec, 2004). It is in such circumstances that preventing critical network events and the shock they bring is critical. By expanding the notion of a 'within system' incident to consider the interdependencies and linkages to real time discontinuities across Type 1 and Type 2 vulnerabilities, an enhanced understanding is possible about the contexts of crises as they go beyond the grasp of competent managerial authorities.

A point to note about network events is that both natural and technological hazards can directly affect human systems, as well as propagated by them. An obvious example of this propagation is the transmission of Sudden-Acute Respiratory Syndrome (SARS) internationally via business and tourist air travel. Similarly the use of the maritime trading system as a vector for terrorism is another.

Research recommendations

A number of viable lines of inquiry should be pursued. The following questions are likely to bring benefit to all stakeholders:

- How will the variable implementation of the CSI and C-TPAT program impact on global sourcing strategies in particular: time-sensitive supply, reliance on single-source or geographical location suppliers?
- Would more complete implementation of the CSI and C-TPAT programs separate countries unable to afford the cost of implementation from access to trade opportunities and thus affect the notion of benign globalisation?

Validation and testing the usefulness of the Type 1 and Type 2 vulnerability construct is also needed, as is an evaluation of the prevalence of crisis management capacities across maritime related industries. Specifically, the following investigations are timely:

- Identifying the generic vulnerabilities in critical infrastructure at major ports from on and off-site sources including the potential for unexpected interaction between infrastructure classes;
- Evaluating the nature of current security risk management and integrated governance systems in place within port-based institutions and the range and depth of training activities currently in place;
- Assessing incidents in the 'high frequency low consequence' and 'low frequency high consequence' categories at these ports - over time thus allowing a descriptive mapping and detailed scoping of Type 1 and Type 2 vulnerability;
- Appraising the potential impact of full integration of port and trade route crisis management capacities on maritime insurance premiums;
- Estimating the cost of enhancing crisis management capacities to industry stakeholders.

A further issue for investigation is the impact of implementing requirements of the ISPS code for ports. A question of particular interest is whether implementation of the ISPS code has simplified or increased operational complexity within a port and among the port-based businesses. Confirmation of a relationship between increasing complexity and vulnerability as implied in the literature could follow in addition to an assessment of changes to on-site security risk management structures and staffing levels. Answers to this issue may allow greater effectiveness in implementation of both CSI and the C-TPAT Initiatives and other wider programs into the future.

9 Conclusion

Assurance of trade security and continuity of supply chains are critical factors in the current global environment. While the conceptual bases for crisis management and related capabilities defined here are well grounded in historical instances of major institutional systems failure and post-crisis learning, there is a need to confirm their suitability and applicability to the task specifications and operational frameworks operating within port and maritime trade settings.

An equally important issue for consideration is the impact of implementing both the treaty mandated ISPS code and voluntary CSI and C-TPAT initiatives at operational ports. A question of particular interest is whether these developments have simplified or increased operational complexity within ports and among the port-based businesses and, across supply chain networks. How these programs are implemented and applied are at the nexus of ensuring security in global supply chains while pursuing business efficiencies. It is arguable that as the post-modern world evolves achieving the former may be at the expense of the latter.

References

Anonymous (2004) *The Rising East: Pirates and Terrorism*, Editorial, [www document] http://www.koreaherald.co.kr/SITE/data/htnl dir/2004/03/05/20403050015.

APEC (2005) Counter-terrorist Action Plans www.apec.org

APEC (2003) *Strengthening International Cooperation and Technical Assistance in Preventing and Combating Terrorism*, Intervention by APEC Secretariat at the 12th Session of the Commission on Crime Prevention and Criminal Justice, 16-19 May, Vienna, Austria.

Barnes, P (2001) *Crisis Management Needs in the Public Sector*, State Conference, Institute of Public Administration Australia Queensland Division, 24 August.

Bateman, S. (2003) 'Maritime Security: A New Environment Following September 11,' in the Symposium of Maritime Experts to Assist in Implementation of the STAR Initiative, Melbourne, 18 – 20 June.

Boin, A. and Lagadec, P. (2000) 'Preparing for the Future: Critical Challenges in Crisis Management,' in the *Journal of Contingencies and Crisis Management*, 8(4): pp. 185-191.

Comfort, L. *et. al.* (2001) 'Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments,' in the *Journal of Contingencies and Crisis Management*, 9(3): pp. 144-157.

Commonwealth of Australia (2003) *Costs of Terrorism (and the benefits of Working Together),* Economic Analytical Unit, Dept. of Foreign Affairs & Trade.

CSCAP (2003) 'Report of the general Conference of the Council for Security Cooperation in the Asia Pacific,' CSCAP, Jakarta, December 7-9.

Fagerberg, J. (1996) 'Technology and Competitiveness,' in the *Oxford Review of Economic Policy,* Vol.12, pp.39-51.

Farrugia, N. (2002) 'Constructing and index of International Competitiveness for Malta,' *Bank of Valletta Review,* No.26, Autumn.

Frittelli, J. F. (2003) *Port and Maritime Security: Background and Issues for Congress*, Congressional Research Service, December 5.

Garelli, S. (2001). 'Competitiveness of Nations: The Fundamentals', *World Competitiveness Yearbook.*

Gooley, T. & Cooke, J. (2002) 'Shippers, carriers struggle with Port shutdowns aftermath,' in *Logistics Management,* November.

Harrald, J. R., Stephens, H. W. and van Dorp, J. R. (2004) 'A Framework for Sustainable Port Security,' *Journal of Homeland security and Emergency Management*, 1(2):1-13.

Hecker, J. Z. (2002) *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*, U.S. General Accounting Office, August 1.

ICS (1990), *Institute of Chartered Shipbrokers, London.* Tutorship *'Ship Sale and Purchase'* Course notes. London 1990.

Janis, I. (1982) Groupthink, Little Brown, Boston.

Jarvis, D. S. L. (2003) *The Arc of Instability: Regional Security Challenges for Australia and the Asia Pacific*, Centre for International Risk, The University of Sydney.

Kumar, S. & Hoffmann, J. (2002) 'Globalisation: The Maritime Nexus,' Chapter 3 in the *Handbook of Maritime Economics,* LLP, London.

Kwek, Keng-Huat & Goswami Nandini. (2004) *Cost and Productivity Implications of Increased Security in Sea Trade Processes* The Logistics Institute-Asia-Pacific. National University of Singapore

Lagadec, P. (2004) 'Crisis: A Watershed From Local, Specific Turbulences, to Global, Inconceivable Crises in Unstable and Torn Environments, Future Crises.' in the International Workshop, Future Agendas: An Assessment of International Crisis Research,

Lagadec, P. and Michel-Kerjan, E. (2004) 'Meeting the Challenge of Interdependent Critical Networks under threat: The Paris Initiative, Anthrax and Beyond,' Cahier No. 2004-014, Laboratoire D'Econometrie, Ecole Polutechnique, Paris.

Langewiesche, W. (2003) **'**Anarchy at sea,' in the *The Atlantic Monthly***,** Sep., 292 (2): pp. 50-70.

Mahon, J.F. and Cochran, P.L. (1991). Fire Alarms and Siren Songs: the role of issues management in the prevention of, and response to, organisational crises. Industrial Crisis Quarterly, 5, pp. 155-176.

Marais, K., Dulac, N. & Leveson, N. (2004) 'Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems,' Presented at the Engineering Systems Division Symposium, MIT, Cambridge, MA, March 29-31.

Mitroff, I.I. & Alpaslan, M.C. (2003) 'Preparing for Evil,' in the *Harvard Business review*, April: 109 -115.

Mitroff, I.I., & Kilmann, R.H. (1984) *Corporate Tragedies: Product Tampering, Sabotage, and other Catastrophes*, Praeger, New York.

Nitsch, V. and Schumacher, D., (2002) 'Terrorism and Trade,' Paper for Workshop *The Economic Consequences of Global Terrorism,* DIW - German Institute for Economic Research, Berlin, June. November 24-26, Sophia-Antipolis (Nice), France.

OECD (2003) *Security in Maritime Transport: Risk factors and Economic Impact*, Maritime Transport Committee, Directorate for Science, Technology and Industry, July.

Pearson, C.M. and Mitroff, I.I. (1993) 'From Crisis Prone to Crisis Prepared: Framework for Crisis Management,' *Academy of Management Executive*, 7(1): pp. 48-106.

Perrow, C. (1984) *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York.

Raby, G. (2003) 'The Costs of Terrorism and the Benefits of Cooperating to combat Terrorism'. *A paper presented by Dr Geoff Raby, Deputy Secretary, Dept of Foreign Affairs and Trade to APEC Senior Officials Meeting, Chiang rai, 21 Feb, 2003 and submitted by Australia to the Secure Trade in the APEC Region (STAR) Conference.*

Rhinard, M., Ekengren M. & Boin, R. (2004) 'Functional Security and Crisis Management Capacities in the European Union: Setting the Research Agenda,' *Research Proposal*, CRC/ Eurosec, 30 May.

Richardson, M. (2004a) 'A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction,' *Viewpoint* - Institute of South east Asian Studies, [www document] www.iseas.edu.sg/viewpoint.

Richardson, M. (2004b) '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, [www document] www.iseas.edu.sg/viewpoint.

Rijpma, J.A. (1997) 'Complexity, Tight-coupling and Reliability: Connecting Normal Accidents Theory and High Reliability Theory,' in the *Journal of Contingencies and Crisis Management*, (5)1: pp. 15-23.

Robertson, D.A. (2004).The Complexity of the Corporation. Human Systems Management (23), pp. 71-78.

Saxton, J. (2002) 'The Economic Costs of Terrorism,' *Joint Economic Committee,* United States Congress, Washington D.C.

Saywell, T. & Borsuk, R., (2002) 'The fallout of the Bali bombings on regional economies: The neighbourhood takes a hit,' *Far Eastern Economic Review,* Hong Kong, 24 October.

Schaad, W. (2002) *'Terrorism-Dealing with the New Spectre,'* Swiss Reinsurance Company Zurich.

Severin, R. C. (2003) 'ASEAN: Security and Development Challenges,' Asian Institute of Management, at the 6th Lecture Series of the Ramos Peace and Development Foundation, Makati, 29 August, [www document], www.iseas.edu.sg/viewpoint/mr5mar04.pdf

Shaw, G.L. and J.R. Harrald, J.R (2004) 'Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Managers,' in the *Journal of Homeland Security and Emergency Management*, Vol. 1: No. 1.

Suárez de Vivero, J & Rodríguez Mateos, J. C. (2004) "New Factors in Ocean Governance: From Economic to Security-based Boundaries," in *Marine Policy*, Vol. 28, pp. 185-188.

The Home Office (2002) *Supply Chain Vulnerability*, Research Report prepared by the Cranfield University School of Management.

Thissen, M. (2004), 'The Indirect Economic Effects of a Terrorist Attack on Transport Infrastructure: a Proposal for a SAGE', *Disaster Prevention and Management: an International Journal,* Vol.13, No.4, pp.315-322.

Turner, B.A. & Pidgeon, N. (1997) *Man-made Disasters (2nd edn*), Butter-worth Heineman, Oxford.

U.S. Dept. of State (2004) Container Security Initiative (CSI) Achieves Major Milestone: 20 of the World's Largest Ports Now Participating with the U.S. in CSI: Port of Piraeus, Greece, is 20th CSI Port to become operational, Office of Public Affairs

U.S. Dept. of Transportation, (2002) Maritime Trade and Transportation, SLSDC EIS, Bureau of Transportation Statistics, [www document] http/www.bts.gov/publications/maritime_trade_and_transportation/2002/index/html.

Van de Voort, M., *et. al.* (2003) *Seacurity (Improving The Security of the Global Sea-Container Shipping System)*, RAND Europe, MR-1695-JRC.

Wilson, J.S, Mann, C. L., Otsuki, T. (2003) *Trade Facilitation and Economic Development: Measuring the Impact*, World Bank Policy Research Working paper 2988, March.