View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Plymouth Electronic Archive and Research Library

Risk Assessment of Maritime Supply Chain Security in Ports and Waterways

Saeyeon Roh[#1], Jason Tam[#2], Sung-Woo Lee[*3], Young-Joon Seo[†4]

[#]*Plymouth Business School, University of Plymouth, United Kingdom*
[1]saeyeon.roh@plymouth.ac.uk
[2]tze.tam@postgrad.plymouth.ac.uk

[*]*Port & Logistics Research Division, Korea Maritime Institute, South Korea*
[3]waterfront@kmi.re.kr

[†]*School of Economics & Trade, Kyungpook National University, South Korea*
[4]y.seo@knu.ac.kr (Corresponding Author)

***Abstract*—Seaports and waterways are crucial for international trade, and damage to them may cost millions to the global economy. In the past, Malaysia has been threatened and attacked by terrorists, and pirates have hijacked ships near the coasts of the Strait of Malacca and the South China Sea. Such acts can negatively affect the country's maritime supply chain. This paper analyses the risk to Malaysia's maritime supply chain security in ports and waterways by applying a risk assessment matrix. The findings show that Malaysian ports are vulnerable to attacks and crime due to various factors. Also, Malaysia's waterways may always be at risk given the country's geographical location and status as one of the most important trade routes in the world. Mitigating the risk to ports and waterways can be accomplished by investing in more advanced security equipment, eliminating corruption, and increasing the military presence in the Strait of Malacca. This study may be able to help to increase ports' policy-makers' preparation and decision-making.**

***Keywords*—** *Maritime supply chain, Seaport, Maritime Logistics, Risk management, Security, Waterways.*

1. Introduction

The terror attacks of September 11, 2001, were a wake-up call for governments, prompting them to strengthen their security in airports and seaports. The attacks resulted in the closure of US airspace and seaports and caused all airplanes to be grounded, halting the movement of goods. In general, the disruption in the supply chain caused problems for businesses. For example, Ford Motors was forced to stop production and assembly lines as lorries loaded with components were delayed at the Mexican and Canadian borders [1].

After 9/11, the US government launched several initiatives, such as the Container Security Initiative (CSI), Customs-Trade Partnership Against Terrorism (C-TPAT), Free and Secure Trade and Operations Safe Commerce to tighten and secure its borders. Even though these initiatives were beneficial to trade security, the international community became quite concerned about how they would impact trade efficiency and cost. The US estimated that the cost of the new security measures would reach approximately 151 billion USD per annum [2]. Furthermore, some of these initiatives require close collaboration with foreign manufacturers and logistics providers to develop secure global supply chains. Under such circumstances, balancing security and efficiency is necessary, and this has generated some problems for managers of domestic and international markets and businesses. Most managers are still very unsure about the actions needed to enhance their respective logistics security programmes [3].

The current rise of global competition in the maritime industry requires much attention from port risk managers due to the increase in terror threats. Proper management of security has become a competitive advantage for companies. Moreover, reducing unexpected losses to maximise overall benefits has also been a factor in securing a competitive advantage. Seaports and the maritime industry are regarded as supply chain components with high uncertainty [4]. A port disruption is defined as an occurrence which causes interruptions to the flow within the transportation system, which may eventually halt the movement of cargo [5]. Such events may cause long delays in cargo flows at seaports, which will have unpleasant effects on various elements of the supply chain.

Port Klang and the Port of Tanjung Pelepas are Malaysia's two major ports. Both are strategically located on one of the busiest sea routes, the Strait of Malacca, which links Northeast and Southeast Asia to Western Europe, Asia and North America. This route is very dangerous as it is threatened by pirates, who can create supply chain disruptions. The Trans-Pacific Partnership (TPP), set up by the US and nine other countries including Malaysia, intends to lower trade barriers to promote and ease the import and export of goods and services. The agreement itself could cover almost 40% of the global economy. There is a need to determine the usefulness of the implemented security initiatives in terms of their completion and efficiency [6]. Any burdensome customs or security measures can influence port operations and maritime supply

Copyright © ExcelingTech Pub, UK (http://excelingtech.co.uk/)

chain efficiency, leading to vast contraction in efficiency and trade [7].

This research examines risk reduction efforts in ports and waterways intended to protect Malaysia's maritime supply chain from terrorism and piracy. Furthermore, it assesses the risks to Malaysia's maritime supply chain security and suggests various improvements. Section 2 reviews the relevant literature. The methodology is presented in Section 3, whilst Section 4 lists the main findings. Concluding remarks are found in Section 5.

2. Literature Review

Managing supply chain risk involves identifying and minimising vulnerabilities by negotiating between members of the chain. Global logistics will always be exposed to collaboration costs, ineffective execution, poor-quality products, supply and demand risks and environmental risks [8]. There is always a trade-off between security and efficiency; therefore, security interruptions have always occurred at various points within the supply chain process, which decreases its efficiency [9]. Willis and Ortiz [10] suggested five capabilities—reliability, efficiency, transparency, resilience and fault tolerance—that help create a high level of security in the global supply chain. Supply chain security takes into account both information and physical flows from the origin point to the customers [11]. Supply chain security management is defined as a function of procedures, policies and forms of technology. It protects the assets of the supply chain (e.g. facilities, equipment, personnel and information) from thievery, damage and terrorism by preventing any unauthorised people, contraband or weapons from entering the chain [12]. Supply chain security involves using policies, procedures and modern technology to prevent illegal acts such as robbery, terror threats and unauthorised acts within the process [13].

As for the maritime industry, its supply chains are very prone to terror attacks and other forms of disturbance due to their complexity and open nature, both nationally and globally [14]. Any form of disruption within the maritime supply chain will have negative implications for the global/local economy and world trade [15]. It has been predicted that any form of disruption in a port will cause 100 billion USD to be lost, with the port closure and recovery cost at around 5.8 billion USD. It will also lead to a domino effect, with the potential for a global economic downturn or the breakdown/disruption of the global supply chain [16]. Being a focal point of global business, the security of ports is arguably the most important way to ensure efficiency and smoothness in every intermodal logistics and supply chain facing ever-increasing complexities [17]. A well-secured port means having a secure supply chain, leading to the smooth movement of goods and proper operation of global business.

The importance of many Asian ports in today's global trade landscape illustrates the need for security. Asian countries must comply with various mandatory international requirements in regard to port security, and one of them is the International Ship and Port Facility Security (ISPS) Code [18]. The ISPS Code, adopted by the International Maritime Organisation (IMO) right after the September 11 attacks, is now the most important international regulation which emphasises the importance of maritime security and provides better protection for port facilities and ships against terrorism [19]. The main purpose of the ISPS Code is to help address weakness or vulnerability in maritime supply chain security which is due to the lack of preventive measures as well as slow responses after an attack; there is basically an ineffective and poor crisis system in place [20]. The code guides and addresses maritime security and supply chains, including ports under the ISPS Code. The main objectives of the code are 1) identifying and detecting any potential security risks; 2) implementing security measures; 3) collecting and providing information in relation to maritime security; 4) providing a reliable method for assessing any maritime-related risk; 5) developing a detailed security plan in the presence of a variable security level; and 6) establishing roles and security in relation to security for ship companies, contracting governments and port operators.

Malaysia implemented the ISPS Code back in 2004, with 500 ships and 80 port facilities having to comply [21]. Legislation regarding the implementation of the code has been incorporated into the 'Merchant Shipping Ordinance' and the Malaysian Marine Department, which is the designated authority, has recommended that each port establish its own security committee. Another international regulation created with the security of supply chains in mind is the C-TPAT, which is a voluntary/government program that works together with Customs and Border Protection (CBD). Both focus on gathering sufficient information on various import shipments to create risk-based examinations as opposed to completely physical inspections and examinations. The C-TPAT regulation reviews the following eight areas of supply chains:

1) Physical security: a) the listing of activities, facilities and hours of operation; b) the installation of security devices,
2) Physical access control: to control access by visitors, employees, vehicles and vendors,

3) Personal security: establish policies when it comes to hiring, verification of citizenship, termination procedures, background checks and employee misconduct,
4) Information security: policies for passwords, user ID, internet access, emails, and hardware and software security,
5) Procedural security: policies for overage and shortages, receiving and shipping hazardous materials, recordkeeping, document viewing, and warehouse security,
6) Security training: policies in relation to the C-TPAT, security and safety training, and any related measures,
7) Conveyance security: policies for the control of containers, the inspection of seals and container storage, and
8) Business partner requirements: policies in relation to selecting, managing and evaluating brokers, suppliers, carriers and warehouses.

The C-TPAT program allows the CBD to work alongside businesses with the purpose of strengthening the international supply chain and improving border security in the US. Malaysia and Singapore already abide by the C-PTAT and have increased their awareness of and protection from disruptions [19]. Ports are relying more and more on the usage of information technology (IT) for various purposes, like communicating with connecting ships, container tracking, and equipment maintenance and management [22]. Technology related attacks on ports can take many forms and often involve the disruption of electricity, which is devastating to energy-reliant ports or terminals. Sabotage can come from employees, a breach in port IT security, or even just an accident due to mishandling of dangerous or hazardous materials [23]. The Baltic and International Maritime Council developed its own advice for countering cyber threats to the shipping industry, which was discussed at the IMO Safety Committee in 2016. Many systems designed before the existence of cybersecurity were running old software on badly designed hardware, and these systems are still running in some container terminals and ports today, increasing the risk of a cyber-attack.

The Strait of Malacca is a major choke point which is vulnerable to disruptions in the maritime supply chain [24]. It is thought that pirates only hijack or attack vessels out on the high seas, but that definition of pirates or piracy is now completely inaccurate, since they are spreading out from the high seas [25]. A staggering 80% of pirate attacks occur within territorial waters and even in ports themselves; such attacks fall outside the definition of piracy and do not qualify under the piracy act of the United Nations 1982 Convention [26]. Disruptions to various supply chains do not only occur within the Strait of Malacca but also within the nearby ports. It is estimated that 146 out of 242 reported piracy attacks occurred within port areas worldwide [18].

The recent ruling by The Hague against China's claims over territories in the South China Sea created uncertainty about the maritime industry and global supply chain. Any form of disruption to the shipping industry within the South China Sea could negatively impact global commerce, including energy supplies [27]. Thousands of vessels pass through the South China Sea every day, as it connects East Asia with the Middle East and Europe, and total yearly trade through the disputed waterway is estimated to be around 5.3 trillion USD [28]. Furthermore, a third of the world's petroleum and liquefied natural gas passes through the Malacca Strait and continues on through the South China Sea [30]. Detouring to avoid conflicts will increase shipping costs, and the maritime industry has expressed concern over the possibility of an increase in insurance rates [6].

3. Methodology

To evaluate and assess the risks to and security of the Malaysian maritime supply chain, this study used a questionnaire survey to collect data. Then, as the main methodology, a risk/loss exposure matrix was employed. A risk/loss exposure matrix is an effective method for evaluating the risk of any type of organisation, firm or supply chain. Yang [30] adopted this method to assess Taiwan's maritime supply chain security. The questionnaire was composed of two sections. The first attempted to determine the importance of security risks in terms of risk frequency and risk severity. The questionnaire used five-point Likert scales to rate risk frequency and risk severity; with regard to risk frequency, see Table 1. The questionnaire was distributed to Port Klang, the Port of Tanjung Pelepas and the Port of Singapore, which are located within the crucial Strait of Malacca. The intended respondents were senior-level managers who worked for terminal operators and port authorities. A total of 178 questionnaires were distributed, and 29 were returned. All respondents were working as senior managers. The alternatives in risk management can be classified by the level of risk exposure: self-retention is utilised for low-level risks; insurance transfers and risk retention for medium risks; loss of control for high-level risks; and non-insurance transfers and risk avoidance for a very intense risk. Exposure avoidance involves making the decision to eliminate a particular operation, activity or asset due to intense risk and

an increased frequency of loss factors. Loss control encompasses both loss reduction and loss prevention; it seeks to reduce the severity of losses after an occurrence. Contract transfer risk is transferrable to anyone, though only through a non-insurance contract or the purchase of insurance. Self-retention includes the expenses related to the loss, unfunded loss reserves, loans taken out to pay for losses, a well-funded loss reserve and utilisation of an insurer.

Table 1. Scale of risk frequency and risk severity

Degree of frequency	Scale	Degree of severity
Very unlikely	1	No disruption
Possible but unlikely	2	Potential minor disruption
Somewhat likely to occur	3	Possibility of moderate disruption
Will be experienced	4	Possibility of disruption
Likely to occur	5	Disruption is likely

Based on a rigorous literature review, the questionnaire was divided into four sections: maritime threats, government intervention, cybersecurity and facility (Table 2).

The current study used a regional case study of the Strait of Malacca including issues of piracy and the South China Sea dispute, unlike previous research that focused on CSI, ISPS and C-TPAT. Sixteen key factors were identified and divided into four sub-factors, equally distributed under piracy and terrorism factors (A1-A4), government intervention (B1-B4), cybersecurity (C1-C4) and facility (D1-D4).

Table 2. Risk assessment factors

Risk assessment factors	References
A. Piracy and Terrorism	
1. Maritime risk control and analysis of the respective port is useful in today's world.	[31]
2. Port and anchorage crimes have always been an issue in ports; such activities always occur in the respective ports.	[32]
3. Terror threats and attacks are very common in today's global environment; the current status of the respective ports makes them vulnerable to such attacks.	[33]
4. The Malacca Strait is considered as one of the most pirate-infested waterways in the world and creates serious operational issues for ports situated nearby.	[32]
B. Government Intervention	
1. Government interventions in the safety and security of pirate-infested waterways have significant impacts and are effective.	[34]
2. Government security regulations and law wills not be enough to counter maritime crime.	[35]
3. The International Ship and Port Facility Security Code was specifically tailored to protect the maritime industry from external threats and is considered effective towards the respective ports.	[21]
4. Collaboration between neighbouring countries to minimize the presence of piracy in the Strait of Malacca is still ongoing and seems to be effective.	[35]
C. Cyber security	
1. We constantly update/upgrade our security network.	[23]
2. We share information regarding threats to neighbouring ports/ government bodies.	[23]
3. Cyber threats are common in today's global environment; there is the possibility of ports' Global Navigational Satellite systems and Global Positioning Systems being disrupted by jammers.	[22]
4. The possibility of ports' information technology systems being hacked and disrupted.	[22]
D. Facility	
1. Security equipment in ports can sometimes be under-utilised. We constantly utilise security equipment in our port.	[36]
2. Only 4% of containers coming into the US are checked via X-rays and physical inspection; the X-ray machines within the respective ports are always fully utilised.	[37]
3. Container flows within the respective ports can be quickly conciliated after a disruption.	[5]
4. The possibility of container theft (seal breakage) within the respective port is high.	[18]

4. Results

Table 3 presents the level of frequency and severity for all three ports analysed. The numbers (risk score) in the table were acquired by multiplying the frequency and severity; for example, 2*2 = 4, 3*4 = 12 and 5*5 = 25. The frequency utilised a scale from 1 = 'strongly disagree' to 5 = 'strongly agree'. The severity also utilised a scale from 1 = 'negligible' to 5 = 'catastrophic'. The table also uses colour coding to illustrate the risk and danger. Table 4 shows the description of each colour and risk. The light grey colour represents a very low risk, which means port operators or authorities view it as an important factor but the possibility of a disruption is fairly low. As for the colour yellow, it represents low risk, which means the possibility of a disruption by any threat can happen at any time, but if it does there is a chance to quickly mitigate losses. Orange represents moderate risk, which means port operators and authorities view it as an important factor, and protecting it is important to operation flows and security. Failure to do so will pose threats which can disrupt supply chain operations. Lastly, the colour red represents high risk. This means that when an accident or issue occurs, a report must be made as soon as possible. Disruption to port operations and the supply chain will happen, and this may influence international trade and port operations negatively to an immense degree. Sufficient time is needed to deal with the disruption.

Table 3. Risk table

		Frequency				
		Strongly Disagree (1)	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
Severity	**Negligible (1)**	1	2	3	4	5
	Minor (2)	2	4	6	8	10
	Moderate (3)	3	6	9	12	15
	Critical (4)	4	8	12	16	20
	Catastrophic (5)	5	10	15	20	25

Source: Authors

Table 4. Risk table description

Risk	Description
Very Low Risk	The odds of a disruption are low but one might occur.
Low Risk	A disruption could happen at any time, and if it does it will be critical to mitigate any losses.
Moderate Risk	Port operators and authorities view this as an important factor; it will fail if a disruption occurs.
High Risk	Report incident immediately. Disruption to the supply chain will no doubt occur and will negatively influence international trade and port operations. Time is needed to conciliate.

Source: Authors

The findings are based on the risk table where each code represents a factor. They were placed in the table to identify which factor was more important and which would have the most consequences if ignored. Table 5 represents Port Klang's risk level. Each key factor of the port was allocated a spot in the risk chart. It can be seen that D2 (X-ray machines are always utilised) is located within the very-low-risk section. Judging from the questionnaire, X-ray machines in Port Klang are underutilised, even though X-ray inspection became a mandatory factor of port standardisation. The port itself does not view it as a risk that the X-ray machines are not in use. Factors A1 (Maritime risk and control analysis is important in today's current global climate), C1 (Constantly upgrade security network) and C4 (Possibility of port IT system being hacked or disrupted) are important, and if overlooked they can cause disruptions to supply chains and operations to an immense degree. Port Klang has decided that these three factors weigh heavily in their minds as they rely on them in their day-to-day operations. In terms of viewing the importance of maritime risk and control, it is known that Port Klang is located very close to one of the most dangerous waterways in the world, the Strait of Malacca. Pirate attacks are known to occur within territorial waters. What is even more frightening is illegal boarding and hijacking of a docked ship, since it is easier to hijack a ship when it is not moving [26]. Assessing their risk and control analysis can provide the port with relevant statistics. As for Port Klang, the possibility of an attack on a ship is high. Accordingly, the port manager or port authority needs to create a contingency, mitigation or prevention plan. Having to rely on technology for everyday operations helps smoothen supply chain flows [38]. The possibility of ports and ships being hacked is still vague, and there have been very few cases. However, knowing that it is possible puts major ports in a position where they need to improve their IT systems. A modern terrorist might not necessarily carry a firearm, but with the right skills and a computer with Internet access, they can disrupt a port's entire operation, halting transportation, disrupting navigation systems and causing delays which will result in an inefficient and slow flow of goods. The other two most important factors for Port Klang relate to its IT security. Port Klang views this factor as an important aspect for the port to operate properly and efficiently. Failing to implement technology can create the possibility of future disruptions. Most cranes and gates in Port Klang are remotely controlled. Someone hacking and taking control of cranes and gates could cause serious disruptions.

Table 5. Risk assessment matrix for Port Klang

		Frequency				
		Strongly Disagree (1)	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
Severity	**Negligible (1)**					
	Minor (2)		D2			
	Moderate (3)			D4 C2 D3	A4	
	Critical (4)			C3	B2 B4 A3 A2 B1 B3 D1	
	Catastrophic (5)					A1 C1 C4

Source: Authors

Table 6. Risk assessment matrix for Port of Tanjung Pelepas

		Frequency				
		Strongly Disagree (1)	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
Severity	**Negligible (1)**					
	Minor (2)					
	Moderate (3)			A4 C2 D1 D2 D3	D4	
	Critical (4)			B4	A2 A3 B1 B3 C3	B2
	Catastrophic (5)				A1 C1	C4

Source: Authors

Table 6 shows the Port of Tanjung Pelepas' risk level. It can be seen that every factor mentioned in the questionnaire is significantly important to their operations and security. The most important one is C4 (possibility of the port's IT system being hacked or disrupted). Much like Port Klang, the port views this factor as an important basis for their operations. The Malaysian government realises that an attack which could disrupt supply chain or container flows would not necessarily come from terrorists or pirates but hackers, who can disrupt everyday operations. That is why the Port of Tanjung Pelepas views this as an important factor which could inevitably cause inconvenience to maritime trade if overlooked.

Table 7 displays the Port of Singapore's risk level. D4 (possibility of container theft or seal breakage) is low in this port, so it does not pose much of a risk to their operations. The Port of Singapore is known to be one of the best ports in the world, and therefore container theft or port crime is relatively low due to Singapore's strict laws, foreign regulations and security. A1 (Maritime risk and control analysis is important in today's current global climate) and C1 (Constantly upgrade security network) are the most important factors for the Port of Singapore. In the current global environment, where terrorism and piracy continue to hold the power to negatively affect world trade, maritime risk and control are greatly needed to ensure the smooth flow and efficiency of supply chains and trade. Therefore, A1 was selected as an important factor which cannot be overlooked due to its ability to create catastrophic disruptions which will influence global trade. For C1, the Port of Singapore views this as an important factor which can cause severe disruptions when overlooked. As a modern port which relies heavily on modern technology, keeping the Port of Singapore's IT system secure is a must if the port wishes to be efficient and on schedule, which in return will ease the movement of containers and the basic supply chain. The Port of Singapore is the world's second busiest port. In order to maintain its efficiency and improve operations, PSA Singapore invested in 22 new automated guided vehicles/cranes with security integration to prevent hackers from hijacking their guided vehicles and have also made efforts to become one of the most technologically advanced ports in the world [39].

Table 7. Risk assessment matrix for Port of Singapore

		Frequency				
		Strongly Disagree (1)	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
Severity	**Negligible (1)**					
	Minor (2)		D4			
	Moderate (3)		C2	A4 D3		
	Critical (4)		A2	A3	B1 B2 B3 B4 C3 D1 D2	
	Catastrophic (5)				C4	A1 C1

Source: Authors

5. Concluding Remarks

Analysing the two Malaysian ports, Port Klang and the Port of Tanjung Pelepas, and the Port of Singapore provided a clear insight into Malaysia's maritime supply chain security. All three ports indicated that government intervention in the safety and security of waterways would no doubt be enough to help protect and counter maritime crime. Government intervention might be very effective at eradicating piracy, but pirates are still very much active in the Strait of Malacca. The ISPS was developed specifically to protect the US, but also poses a positive externality by providing ports around the world with another layer of security. There is a debate on whether the ISPS can really prevent potential hijacks [40]; it can better secure ports, but also it was found that it is relatively difficult to protect inbound and outbound ships.

The three port authorities agreed that when a disruption occurs it can be difficult to manage resources and recover. Having up-to-date machinery, software and security equipment can help prevent disruptions and mitigate losses. Disruptions in ports can create bottlenecks for the maritime supply chain industry resulting from inefficiency, slow supply chain flows and delayed transportation. The recovery time will depend on the severity of the damage. Port and anchorage crime is high in Malaysian ports, and these could be influenced by corruption, poor management and poor resource planning. There are some reports of corruption, such as selling identification cards and passports, which has existed in the immigration field for a long time. Malaysian ports located in the Strait of Malacca are always vulnerable to pirates. They have strengthened their partnerships with other nations to improve port security through the implementation of ISPS, C-TPAT and the CSI. Maintaining partnerships with other nations may be enough for Malaysia to enhance their security, but investing in high-end security equipment and employing port personnel who integrate good faith with work ethics are advised. Information sharing is crucial to preventing security flaws or attacks that could jeopardise the entire industry. However, poor implementation could bring about a higher risk of attacks, as information may be sold to pirates [41]. Such activities will pose threats to shipping lanes, ships and crews. Regarding the possibility of container theft and seal breakages, Port

Klang was neutral and the Port of Tanjung Pelepas signified this as a significant threat. On the other hand, the Port of Singapore showed little concern about this issue. The Malaysian ports showed different perspectives on container theft due to their proximity to the Strait of Malacca.

Given the TPP trade agreement and China's claims to parts of the South China Sea, there will surely be uncertainty when it comes to the security of the waterways. Training and development for port employees is also needed, specifically in regard to ethics in the working environment and in the process of trying to reduce corruption. Piracy can be controlled through sharing intelligence/information, collaborating with neighbouring countries, increasing military spending and deploying more naval forces in the Strait of Malacca. The increase in international trade could attract pirate attacks that will disrupt the supply chains for Malaysia and other countries.

The maritime security of Port Klang is related to various factors such as the utilisation of X-ray machines, which were found to be underutilised due to a lack of skilled employees. The global environment, frequent upgrades to security networks and the possibility of cyber-attacks on the port were also considered important to the maritime supply chain. The possibility of the IT system being disrupted was regarded as the most serious high-risk factor for the Port of Tanjung Pelepas. The Port of Singapore had strict security and regulations, and it abided by the ISPS Code. They have prepared for an increase in cyber threats and intend to protect their data, automated machines and operations, as they rely heavily on automated machines. Thus, upgrades to the port's security networks are necessary to prevent unauthorised access to important information. Malaysia's waterways are one of the most important trade routes for the maritime industry. Malaysia needs to increase its military/naval presence in the Strait of Malacca and parts of the South China Sea. Also, corruption needs to be eliminated to pave the way for information and intelligence sharing with neighbouring countries. One of the limitations of this research is that data were collected from only some of the ports located in the Strait of Malacca. Therefore, this study could be expanded on by future research that broadens the focus to other geographical locations, such as Africa.

References

[1] Juttner, U., "*Supply Chain Risk Management: Understanding the Business Requirements from a Practitioner Perspective*". The International Journal of Logistics Management, Vol. 16, No. 1, 120-141, 2005.

[2] Bernasek, A., "*The Friction Economy: American Business Just Got the Bill for the Terrorist Attacks, $151 Billion – A Year*", Fortune, Vol. 145, pp. 104-111, 2002.

[3] Bud, B.J., "*Security: The Shipper Speaks*", Supply Chain Management Review, Vol. 6, No. 6, pp. 9-12, 2002.

[4] Seo, Y.-J., Dinwoodie, J., Roe, M., "*The Influence of Supply Chain Collaboration on Collaborative Advantage and Port Performance in Maritime Logistics*", International Journal of Logistics: Research and Applications, Vol. 19, No. 6, pp. 562-582, 2016

[5] Wilson, M.C., "*The Impact of Transportation Disruptions on Supply Chain Performance*", Transportation Research Part E: Logistics and Transportation Review, Vol. 43, No. 4, pp. 295-320, 2007.

[6] Barnes, P., Oloruntoba, R., "*Assurance of Security in Maritime Supply Chains: Conceptual Issues of Vulnerability and Crisis Management*", Journal of International Management, Vol. 11, No. 4, pp. 519-540, 2005.

[7] Wilson, J.S., Mann, C.L., Otsuki, T., *Trade Facilitation and Economic Development: Measuring the Impact*, World Bank Policy Working Paper, 2003.

[8] Seo, Y.-J., Dinwoodie, J., Roe, M., "*Measures of Supply Chain Collaboration in Container Logistics*", Maritime Economics & Logistics, Vol. 17, No. 3, pp. 292-314, 2014.

[9] Harland, C., Brechley, R., Walker H., "*Risk in Supply Networks*", Journal of Purchasing and Supply Management, Vol. 9, No. 2, pp. 51-62, 2003

[10] Willis, H.H., Ortiz, D.S., "*Evaluating the Security of the Global Containerized Supply Chain*", RAND Corporation, 2004.

[11] Banomyong, R., 2005, "*The Impact of Port and Trade Security Initiatives on Maritime Supply Chain Management*", Maritime Policy Management, Vol. 32, No. 1, pp. 3-13, 2005.

[12] Closs, D.J., McGarrel, E.F., "*Enhancing Security Throughout the Supply Chain*", IBM Centre for the Business of the Government, 2004.

[13] Tang, C, "*Perspective in Supply Chain Risk Management*", International Journal of Production Economics, Vol. 103, No. 2, pp. 451-488, 2006.

[14] Van de Voort, M., O'Brien, K.A., Rahman, A., Valeri, L., 2003 "*Seacurity: Improving the Security of the Global Sea-Container Shipping System*", RAND Corporation, 2003.

[15] Saxton, J., *The Economic Costs of Terrorism*, Joint Economic Committee. United States Congress, Washington D.C., 2002.

[16] Greenberg, M.D., Chalk,P., Willis., H.H., Khiko, I., Ortiz, D.S., *Maritime Terrorism: Risk and Liability*, Santa Monica: RAND, 2006

[17] Ng, K.Y.A., "*Port Security and the Competitiveness of Short Sea Shipping in Europe: Implications and Challenges*", in K. Bichou, M.G.H. Bell and A. Evans (eds.), *Risk Management in Port Operations, Logistics and Supply Chain Security*, London: Informa, pp. 347-366, 2017.

[18] Talley, W., *Maritime Safety*, London: Informa, 2008.

[19] Sheu, C., Lee, L., Niehoff, B., "*A Voluntary Logistics Security Program and International Supply Chain Partnership*", Supply Chain Management: An International Journal, Vol. 11, No. 4, pp. 363-374, 2006.

[20] U.S Customs and Border Protection, *C-TPAT's Five Step Risk Assessment*, 2016.

[21] Australian Maritime Safety Authority, *Implementation of the ISPS Code in Malaysia*, 2016.

[22] Polemi, D., Ntouskas, T., Georgakakis, E., Douligeris, C., Theoharidou, M., Gritzalis, D., "*S-Port: Collaborative Security Management of Port Information Systems*", IISA 2013 Conference, 2013

[23] Caponi, S., Belmont, K., *Maritime Cybersecurity: A Growing Threat Goes Unanswered*, BlackRomeMaritime, 2014

[24] Marlow, P., "*Maritime Security: An Update of Key Issues*", Maritime Policy & Management, Vol. 37, No. 7, pp. 667-676, 2010

[25] Dillon, D., "*Maritime Piracy: Defining the Problem*", SAIS Review, Vol. 25, No. 1, pp. 155-165, 2005.

[26] Bendall, H.B., "*Cost of Piracy: A Comparative Voyage Approach*", Maritime Economics & Logistics, Vol. 12, No. 2, pp. 178-195, 2010.

[27] Thekdi, S.A., Santos, J., "*Supply Chain Vulnerability Analysis Using Scenario-Based Input-Output Modelling: Application to Port Operations*", Risk Analysis: An International Journal, Vol. 36, No. 5, pp. 1025-1039, 2016.

[28] Pillai, K.V, Raisah, R., Williams, G., "*The impact of Trans Pacific Partnership (TPP) Agreement on US and Malaysian Business' Foreign Labour Practices*", Procedia – Social and Behavioral Sciences, Vol. 219, pp. 589-597, 2016.

[29] Rusli, M., "*The Application of Compulsory Pilotage in Straits Used for International Navigation: A Study of the Straits of Malacca and Singapore*", Asian Politics & Policy, Vol. 3, No. 4, pp. 501-526, 2011.

[30] Yang, Y.C., "*Risk Management of Taiwan's Maritime Supply Chain Security*", Safety Science, Vol. 49, No. 3, pp. 382-393, 2011.

[31] Kwesi-Buor, J., Menachof, D., Talas, R., "*Scenario Analysis and Disaster Preparedness for Port and Maritime Logistics Risk Management*", Accident Analysis & Prevention, 2016

[32] Eski, Y., "*Port of Call: Towards a Criminology of Port Security*", Criminology and Criminal Justice, Vol. 11, No. 5, pp. 415-431, 2011

[33] Rusca, F., Rosca, E., Rusca, A., Rosca, M., Burciu, S., "*The Influence of Transport Network Vulnerability for Maritime Ports*", IOP Conference Series: Materials Science and Engineering, 2015.

[34] Baniela, S.I., Rios, J.V., 2012, "*Piracy in Somalia: A Challenge to the International Community*", Journal of Navigation, Vol. 65, No. 4, pp. 693-710, 2012

[35] Priddy, A. and Casey-Maslen, S., "*Counter-Piracy Operations by Private Maritime Security Contractors – Key Legal Issues and Challenges*", Journal of International Criminal Justice, Vol. 10, No. 4, pp. 839-856, 2012.

[36] McLay, L., Dreiding, R., "*Multilevel, Threshold-based Policies for Cargo Container Security Screening Systems*", European Journal of Operational Research, Vol. 220, No. 2, pp. 522-529, 2012.

[37] Bier, V.M, Haphuriwat, N., "*Analytical Method to Identify the Number of Containers to Inspect at US Ports to Deter Terrorist Attacks*", Annals of Operations Research, Vol. 187, No. 1, pp. 137-158, 2009.

[38] Kwak, D.-W., Seo, Y.-J., Mason, R., "*Investigating the Relationship between Supply Chain Innovation, Risk Management Capabilities and Competitive Advantage in Global Supply Chains*", International Journal of Operations & Production Management, Vol. 38, No. 1, pp. 2-21, 2018.

[39] Espina, K., *PSA Singapore Invests in 22 New Automated Guided Vehicles*, Lloyd's List, 2016

[40] Missing Malaysian Oil Tanker Found in Indonesian Waters, https://edition.cnn.com/2016/08/17/asia/oiltanker/hijacking/index.html, Last access (05-02-2018).

[41] Pirates in Southeast Asia: The World's Most Dangerous Waters, http://time.com/piracy-southeast-aisa-malacca-strait/, Last access (06-02-2018)