CyRiM Report 2019

Shen attack
Cyber risk in Asia Pacific ports

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
LLOYD'S
AON Empower Results®
MSIG
SCOR The Art & Science of Risk
TransRe We value risk.
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School

About CyRiM

Cyber risks are emerging risk with new complexities that call for insurers and risk managers to jointly develop innovative solutions and tools and enhance awareness and underwriting expertise.

The Cyber Risk Management (CyRiM) project is led by NTU-IRFRC in collaboration with industry partners and academic experts. CyRiM is a pre-competitive research project that aims to foster an efficient cyber risk insurance market place through engaging industry and academic experts guided by government and policy level research. The CyRiM project will help Singapore become an industry centre of excellence on cyber risk and grow the cyber risk insurance market by promoting both the demand and the supply of insurance coverage.

For more information about CyRiM please visit
http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx

CyRiM disclaimer

This report has been co-produced by Lloyd's, Aon, MSIG, SCOR, TransRe and CyRiM for general information purposes only. This does not reflect the views of the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre and additionally does not necessarily reflect the views of any CyRiM partners. While care has been taken in gathering the data and preparing the report and the information herein, Lloyd's, CyRiM, the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre and the Cambridge Centre for Risk Studies do not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied. Lloyd's, Aon, MSIG, SCOR, TransRe, the Nanyang Technological University of Singapore Insurance Risk and Finance Research Centre, CyRiM and the Cambridge Centre for Risk Studies accept no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

About Cambridge Centre for Risk Studies

The Centre for Risk Studies is a world leading centre for the study of the management of economic and societal risks. The Centre's focus is the analysis, assessment, and mitigation of global vulnerabilities for the advancement of political, business, and individual decision makers.

The Centre provides frameworks for recognizing, assessing, and managing the impacts of systemic threats. The research programme is concerned with catastrophes and how their impacts ripple across an increasingly connected world with consequent effects on the international economy, financial markets, firms in the financial sectors, and global corporations. To test research outputs and guide new research agendas, the Centre engages with the business community, government policy makers, regulators, and industry bodies.

Cambridge Centre for Risk Studies disclaimer

This report describes a hypothetical scenario developed as a stress test for risk management purposes. It is not a prediction. The Cambridge Centre for Risk Studies develops hypothetical scenarios for use in improving business resilience to shocks. These are contingency scenarios used for 'what-if' studies and do not constitute forecasts of what is likely to happen.

The views contained in this report are entirely those of the research team of the Cambridge Centre for Risk Studies, and do not imply any endorsement of these views by the organisations supporting the research, or our consultants and collaborators. The results of the research presented in this report are for information purposes only. This report is not intended to provide a sufficient basis on which to make an investment decision. The Centre is not liable for any loss or damage arising from its use. Any commercial use will require a license agreement with the Cambridge Centre for Risk Studies.

Key contacts

Trevor Maynard
Head of Innovation, Lloyd's
trevor.maynard@lloyds.com

Shaun Wang
Project Lead, CyRiM
shaun.wang@ntu.edu.sg

For general enquiries about this report and Lloyd's work on emerging risks, please contact
innovation@lloyds.com

Cambridge Centre for Risk Studies

Research team:
- Dr Jennifer Daffron, Research Associate
- Kelly Quantrill, Research Assistant
- Jennifer Copic, Research Associate
- Kayla Strong, Research Assistant
- Simon Ruffle, Director of Research and Innovation
- Dr Andrew Coburn, Director of Advisory Board
- Timothy Douglas, Research Assistant
- Eireann Leverett, Senior Risk Researcher
- James Bourdeau, Research Assistant
- Oliver Carpenter, Research Assistant
- Tamara Evan, Research Assistant
- Ken Deng, Research Assistant
- Professor Danny Ralph, Academic Director
- Dr Michelle Tuveson, Executive Director

Report citation:

Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University, *Shen attack: Cyber risk in Asia Pacific ports*, 2019

Or

Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K., Leverett, E., Cambridge Centre for Risk Studies, *Shen attack: Cyber risk in Asia Pacific ports*, 2019

Insurance industry interviews and consultation
- Ed Messer, Aon
- Andrew Mahony, Aon
- Lauren Clarke Wiest, Aon
- Alan Godfrey, Axis Capital
- Joe Mellen, Antares
- John Moore, Delta Insurance
- Jasper Hartono, Delta Insurance
- Matt Harrison, Hiscox
- Kara Owens, Markel
- Guenter Kryszon, Markel
- John Brice, MSIG
- Lucien Mounier, Beazley
- Sebastien Heon, SCOR
- Grace Lim, TransRe
- Rhett Hewitt, TransRe
- Lauren Markowski, TransRe

Lloyd's project team
- Dr Trevor Maynard, Innovation
- Anna Bordon, Innovation
- Kieron Price, Innovation
- Angela Kelly, Commercial
- Pavlos Spyropoulos, Commercial
- May Chen, Commercial
- Amy Fu, Commercial
- Linda Miller, Global Marketing
- Sharonjeet Meht, Global Marketing
- Flemmich Webb, External Communications
- Nathan Hambrook-Skinner, External Communications
- Albert Kuller, Class of Business
- Guy Sellers, Class of Business
- Christian Stanley, Class of Business
- Chris Murlowski, Class of Business

Lloyd's Market Association
- Patrick Davison, Deputy Director, Underwriting
- Phil Norwood, Senior Executive, Underwriting
- Tony Elwood, Senior Executive, Underwriting
- Gary Budinger, Senior Executive, Finance and Risk

Nanyang Technological University – Insurance Risk and Finance Research Centre (NTU-IRFRC)
The Centre is established at the Nanyang Business School (NBS), Nanyang Technological University, Singapore. It aims to promote insurance and insurance related risk research in the Asia Pacific. It is seen as a key foundation to establishing dialogue between the industry, regulators and institutions, and sharing critical knowledge to facilitate the growing role of the insurance industry in the economic development of the region.

Further thanks go to the remaining cyber experts who wish to remain anonymous.

Contents

About CyRiM

The Cyber Risk Management (CyRiM) project is led by Nanyang Technological University – Insurance Risk and Finance Research Centre (NTU-IRFRC) in collaboration with industry partners and academic experts including the Cambridge Centre for Risk Studies. CyRiM is a pre-competitive research project that aims to foster an efficient cyber risk insurance market place through engaging industry and academic experts guided by government and policy level research. The CyRiM project will help Singapore become an industry centre of excellence on cyber risk and grow the cyber risk insurance market by promoting both the demand and supply of insurance coverage.

Scope

The project initially considered all cyber related insurance risks such as data breach, property damage, personal injury and loss of life, liability, reputation damage, infrastructure damage, and terrorism. However, for effective data analytics, the project's scope was refined through identification and selection of those risks considered insurable and suitable for further actuarial modelling. The full range of risks are considered in the cyber event scenarios.

The CyRiM project is based in Singapore and has a strong focus on building local capabilities relating to cyber risk while also maintaining a global perspective with hubs in the US and Europe.

Problem statement

The real and present danger posed by cyber risk to businesses and society needs to be tackled on multiple levels. Insurance is one important component in managing this rapidly growing threat as it can provide risk mitigation and transfer. However, the insurance industry is improving the understanding of the unique, complex and evolving nature of cyber risk to provide a robust cyber insurance cover required by those at risk.

The lack of sound data, the rapidly changing cyber threat environment, developing regulation and policy landscape, and the global nature of cyber risk with potential for high accumulation risk, constrains the development of the current cyber risk insurance market.

Objectives

- Research into the definition of cyber risk with the aim of delivering an appropriate classification that also considers the emerging cyber information risk landscape and jurisdiction variations.
- Creation of a cyber related event loss data-set including analysis of risk drivers and translation to estimated insurance claims based on a standardised set of defined contract wordings.
- Creation of a set of cyber event scenarios for impact quantification and study of accumulation risk in systemic events.
- Creation of benchmark cyber loss models and dependency information to support actuarial pricing.
- Collaborative development of a non-intrusive cyber security exposure assessments capability to support company rating and integration with underwriting processes.

Governance and funding

- Aon
- Lloyd's of London
- MSIG
- SCOR
- TransRe

The project is overseen by a Project Oversight Board consisting of representatives of Monetary Authority of Singapore (MAS), Cyber Security Agency of Singapore (CSA), NTU-IRFRC and the industry Founding Members.

Executive summary

What would the impact be on the global economy and insurers if several ports in Asia-Pacific were forced to close as a result of a cyber-attack?

This report seeks an answer to this question by exploring the impact of a hypothetical computer virus, Shen - from the Chinese mythological clam monster, used maliciously against a port management system which closes up to 15 ports across several Asia-Pacific countries.

While cyber-attacks have impacted individual ports in the past, an attack on systemic vulnerabilities across ports on this scale has never been seen. However, the combination of aging shipping infrastructure and globally complex supply chains, makes the shipping industry vulnerable to extreme losses. This attack takes advantage of a vulnerability in port management software provided by a prominent hypothetical ship management company, which manages hundreds of ships.

The narrative of this attack is especially useful because it reveals the complex marine cargo management supply chain and exposes the potential threat posed by insecure third-party suppliers.

The scenario presents three variants of increasing losses, with all results reflecting low probability, high impact situations. The S1 scenario variant affects ports located in Japan, Malaysia, and Singapore. The S2 scenario variant adds The Republic of Korea to the affected countries of S1. The X1 scenario variant adds China, the world's largest shipping export country, to the affected countries in the previous variants for a total of 15 ports affected.

Box 1: Key findings

- Economic damage to the world economy from a concerted global cyber-attack on 15 Asian ports may range from between $40.8 billion (in the least severe scenario variant, S1) to $109.8 billion (in the most severe scenario variant, X1).
- The sectors that suffer the heaviest direct and indirect economic losses are Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction.
- Productivity losses affect each country that has bilateral trade with the attacked ports. Asia would be the worst affected region, set to lose up to $26bn in indirect economic losses, followed by $623m in Europe and $266m in North America.
- The total claims paid by the insurance industry is estimated at $3.6 billion for S1 to $8.3 billion for X1.
- Insurance industry losses are between 8% and 9% of the total economic loss, which shows there are high levels of underinsurance for this type of cyber-attack.
- Business Interruption and Contingent Business Interruption coverages are the main drivers of the insured losses (63% of total losses for S1, 60% for X1).
- Non-affirmative cyber, meaning that cyber is not explicitly mentioned in the policies, accounts for 62% of the total insured losses in S1 and 57% in X1.
- In scenario variant X1 port operators will carry 50% of the insured losses.

Table 1: Economic losses from the hypothetical Shen attack on port management systems in the Asia-Pacific region by scenario variant

Scenario variant	Countries with ports directly affected	Number of ports affected	Total economics losses ($bn)	Direct economic losses ($bn)	Indirect Economic losses ($bn)
S1	Japan, Malaysia, Singapore	6	$40.8	$25.7	$15.1
S2	Japan, Malaysia, Singapore, The Republic of Korea	9	$55.9	$36.8	$19.1
X1	Japan, Malaysia, Singapore, The Republic of Korea, China	15	$109.8	$83.7	$26.1

Values have been rounded to the nearest whole number.

This is a deterministic scenario. The University of Cambridge Centre for Risk Studies (CCRS) is not attempting to put uncertainty or probability to the values presented in this report. A series of events is assumed, for which specific outcomes are assigned. The detailed loss estimates shown are a result of the granularity of the calculation process. Figures presented are potential estimates, not the projected outcome. This is an appropriate approach for a deterministic outlook involving multiple threats in a clash event.

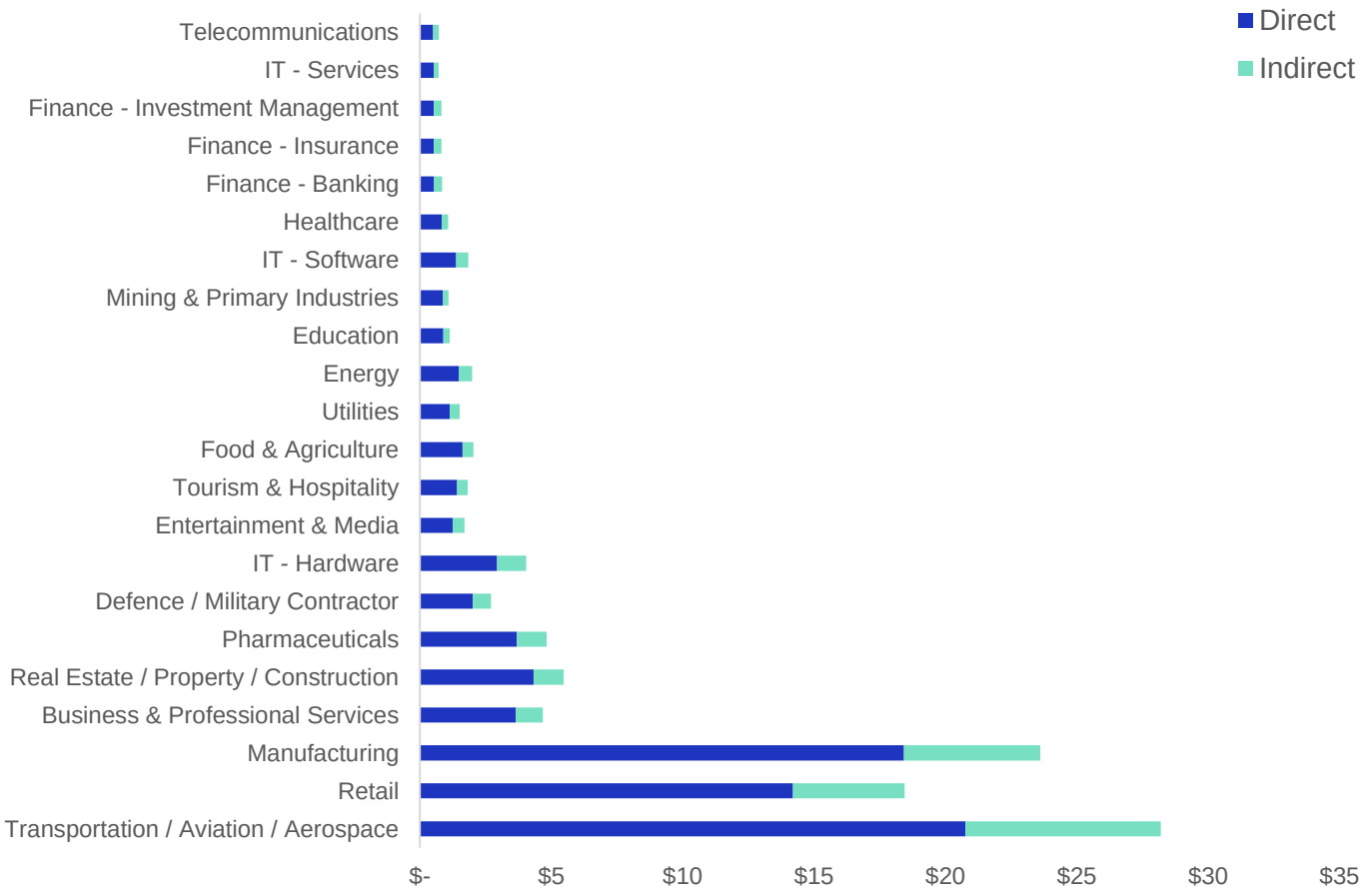
For the purposes of this scenario, ports in the Asia-Pacific are no more vulnerable to the Shen virus than ports in other parts of the world. Asian ports are affected, and these impacts are modelled, because they are targeted directly by the Shen virus. If the attackers had chosen to focus their efforts on ports in the United States, for example, then similar vulnerabilities and impacts would be seen, but insurance losses could be higher in certain classes.

'Shen attack: Cyber risk in Asia Pacific ports' is the second of two joint reports produced by the Cyber Risk Management (CyRiM) project led by Nanyang Technological University, in collaboration with industry partners and academic experts including the Cambridge Centre for Risk Studies. CyRiM industry founding members include Aon, Lloyd's - the specialist insurance and reinsurance market, MSIG, SCOR, and TransRe.

Economic losses by industry sector and countries

The scenario shows the economic damage to the world economy from a concerted global cyber-attack on 15 Asian ports may range from between $40.8 billion (in the least severe scenario variant, S1) to $109.8 billion (in the most severe scenario variant, X1).

Figure 1: Total global direct and indirect economic losses by sector for scenario variant X1



Direct economic losses

Economic losses mount from direct losses due in part to perishables and delayed delivery of goods, with most of the losses stemming from business interruption from port closures. Indirect losses flow through the global maritime supply chain reaching across the world. All sectors are impacted by the scenario, but the sectors that suffer the heaviest direct and indirect economic losses are Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction. These sectors are heavily reliant on economic input from the Transportation sector. The impacts from port closures will be global.

- Port closures in Japan will directly affect the USA, China, the Republic of Korea, the Republic of China (ROC) and Hong Kong Special Administrative Region of the People's Republic of China. In 2017, 32% of Japan's exports to the USA were cars and 7.2[1]% of their exports to China were electronic integrated circuits, indicating a significant impact to the Manufacturing sector in these trade partner countries.
- Malaysia's top maritime trading partners, Singapore, China, the USA, Japan, and Thailand will be adversely affected by any restriction to day-to-day shipping functions.
- The closure of the port in Singapore will affect China, Hong Kong Special Administrative Region of the People's Republic of China, Malaysia, the USA, and Indonesia. In 2017 Singapore's primary exports to China were predominantly electronic integrated circuits (40%) and refined petroleum oils (7.5%),[2] so Manufacturing and IT - Hardware will suffer severely in this scenario.

[1] The Observatory of Economic Complexity 2017

[2] The Observatory of Economic Complexity 2017

- Ports' shutdown in The Republic of Korea will have a significant impact to their top five exporting markets of China, USA, Vietnam, Hong Kong Special Administrative Region of the People's Republic of China, and Japan. 31% of their exports to China in 2017[3] were electronic integrated circuits, so any constraints placed on the shipment of these goods would have negative implications for the Manufacturing sector in particular.
- The international reach of port closures in China will be experienced throughout the world with the countries of USA, Hong Kong Special Administrative Region of the People's Republic of China, Japan, The Republic of Korea, and Vietnam suffering highest direct losses from the closures.

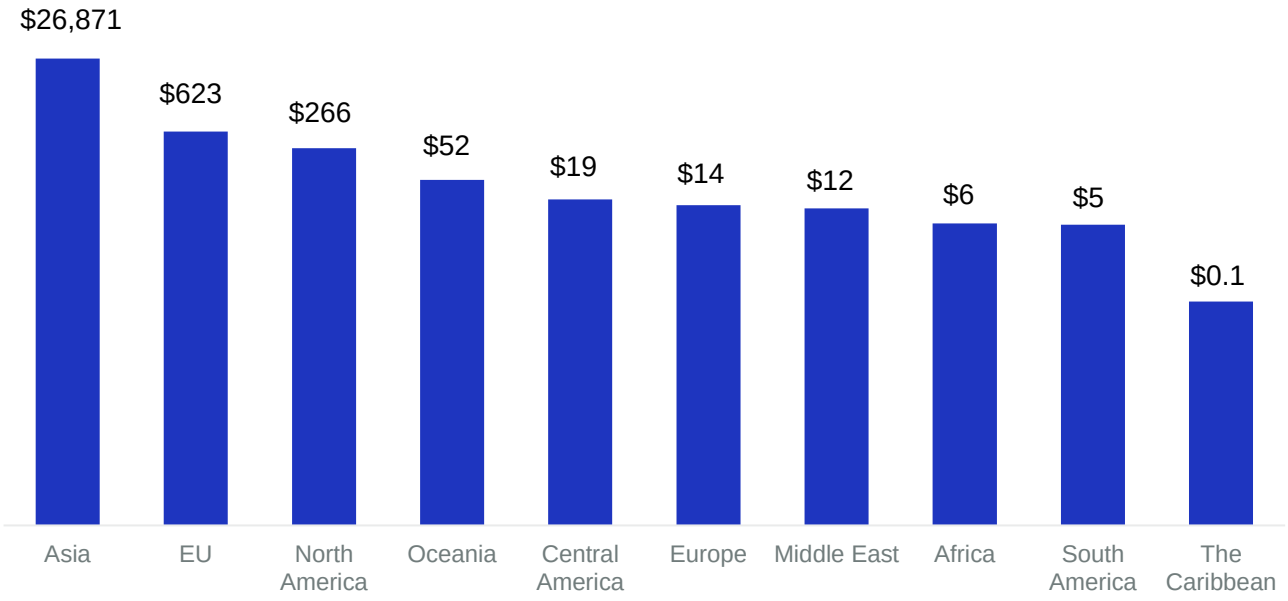
Indirect economic losses

Although the Shen virus only directly affects ports in the Asia Pacific region, economic losses are felt around the world from this scenario due to the global nature of the maritime supply chain.

The indirect losses modelled in this scenario are the productivity losses for each country that has bilateral trade with the affected ports in their respective countries. A daily loss is calculated for each affected country based on the GDP, merchandise trade, world container share percentage, country exports,[4] and bilateral trade index of the 155 countries for which data is available.[5]

Productivity losses affect each country that has bilateral trade with the attacked ports. Asia would be the worst affected region, set to lose up to $110bn in indirect economic losses, followed by $816m in Europe and $348m in North America.

Figure 2: Total indirect losses by region ($million)



In this figure a logarithmic scale is applied to account for the large differences across territories.

The indirect losses presented in this report are cautious estimates. Though they have been modelled extensively, they are not modelled through all levels of the supply chain. For example, the direct impact to ports in China is expected to impact the US economy. This has been modelled and these losses are included in the report. However, the tertiary impact that the impact to the US economy has is not modelled. As a result, the indirect losses shown here can foreseeably be significantly higher as the impacts compound through multiple supply chain tiers.

[3] The Observatory of Economic Complexity 2017
[4] World Integrated Trade Solution 2017
[5] UNCTADstat 2018a

Insurance losses

The report also analyses the implications of these direct and indirect consequences on insurance losses. The scenario shows that during and after such an attack insurance claims would be made for Business Interruption, Contingent Business Interruption, Directors and Officers, Marine Cargo, Technology Errors and Omissions, Regulatory and Defence Coverage, Data and Software Loss, Incident Response costs and Reputational Risk. Notably, not all jurisdictions or insurers recognise data as property. Losses highlighted in this report may vary and policyholders should always check with their insurer definitions and exclusions.

The total claims paid by the insurance industry is estimated at $3.6 billion for S1 to $8.3 billion for X1. Comparing the insurance loss estimates to the economic losses shows insurance industry losses are between 8% and 9% of the total economic loss, which shows there are high levels of underinsurance for this type of cyber-attack. This is driven by low levels of cyber insurance penetration and policy limit structures that were frequently unable to support the scale of losses modelled in this scenario. Close examination of these results indicates that Business Interruption and Contingent Business Interruption (CBI) coverages are the main drivers of the insured losses (63% of total losses for S1, 60% for X1). In this report, indirect economic losses are estimated at a country level via supply chain impacts, focusing on countries with close trading relationships to the affected countries. This loss then flows into an insurance model of the level of CBI coverage available within each country. CBI insurance is complex and challenging to model, further research on the topic is required.

Table 2: Total economic and insurance losses by scenario variant

Scenario variant	Countries	Total economic losses ($bn)	Insured losses ($bn)	Uninsured losses ($bn)	Insurance loss as a % of economic loss
S1	Japan, Malaysia and Singapore	$40.8	$3.6	$37.2	8.8%
S2	+ The Republic of Korea	$55.9	$4.9	$60	8.9%
X1	+ China	$109.8	$8.3	$101.6	7.5%

Values have been rounded to the nearest whole number.

Affirmative' and 'non-affirmative' cyber insurance losses

The report also analyses the impacts of the scenario on 'affirmative' and 'non-affirmative' cyber insurance losses (standalone cyber policies and cyber endorsements on traditional policies are considered affirmative cyber insurance, while traditional policies without explicit exclusions are considered non-affirmative).

The scenario shows that during and after such an attack insurance claims would be made for Business Interruption, Contingent Business Interruption, Reputation Risk, Incident Response Costs, Regulatory Defence Coverages, and Liability risks. Non-affirmative cyber accounts for 62% of the total insured losses in S1 and 57% in X1. Port Management System and Ship Owners will see all their losses (7% of the total) from non-affirmative cyber.

Types of companies that would make claims

These are the primary categories of policyholders that would make claims in this scenario:

– Port Operators

- Port Operators are defined as companies or boards who regulate and manage port and marine services, facilities, and activities within their associated jurisdictional waters.
- In scenario variant X1 port operators will carry 50% of the total insured losses of which 63% will be under an All Risks policy (non-affirmative cyber).

– Third-Party Organizations Indirectly Impacted

- Third-party organizations who are indirectly impacted include those who are impacted further along the supply chain.
- In scenario variant X1, Third-Party Organizations Indirectly Impacted (Supply Chain Companies) will carry 21% of the total insured losses of which 89% will be under an All Risks policy (non-affirmative cyber).

– Logistics and Cargo Handling Companies

- Logistics and Cargo Handling Companies are responsible for the planning, execution and control of the movement of cargo and goods, information, and services. Logistics and Cargo Handling Companies connect the marine cargo industry with wider supply chains.
- In scenario variant X1 Logistics and Cargo Handling Companies will carry 16% of the total insured losses of which 65% will be under an All Risks policy (non-affirmative cyber).

– Perishable Cargo Content Owners

- The cargo content owners are either individuals or organisations that have paid for cargo under a legal contract. It is assumed that roughly 7% of the cargo turnover is perishable and has spoilage due to shipping delays.
- In scenario variant X1 cargo content owners will carry 3% of the total insured losses, all affirmative.6

– Ship Owners

- Ship owners are the individuals or organisations responsible for the ownership and operation of the vessel.
- In scenario variant X1 ship owners will bear less than 1% of the total insured losses, all non- affirmative.

– Port Management System

- The Port Management System is a software application that supports the administration and operations of port operators in a range of tasks.
- In scenario variant X1 port operators will carry 6% of the total insured losses, all non- affirmative

– Ship Management Company

- A Ship Management Company is a company independent of the owner of the ship which maintains and operates the vessel.
- In scenario variant X1 the Ship Management Company will carry 3% of the total insured losses of which 87% will be under an All Risks policy (non-affirmative cyber).

Conclusions

The maritime supply chain is a complex system of interconnected economies. There is no doubt that technology has improved the shipping industry allowing for better tracking, management, and just-in-time deliveries, however, aging ships are a problem. Many vessels at sea are over thirty years old and were not designed with cyber in mind. Responding to these challenges is therefore critical for the well-being of the maritime industry and those who insure it.

Many sectors would be affected across the world with the largest losses arising from the Transportation / Aviation / Aerospace, Retail, Manufacturing, and Real Estate / Property / Construction sectors. This report highlights the current insurance gap for the marine industry where 92% of the economic losses in the extreme version of the scenario are uninsured. Finally, systemic cyber vulnerabilities can have a catastrophic effect on the global supply chain, stemming from the directly affected country or sector with contingent business interruption identified as particularly damaging.

However, there are also opportunities for insurers to grow their business in the insurance classes associated with the Shen Attack scenario. For example, Asia is one of the fastest-growing markets for cyber insurance. The market saw an 87% increase in cyber insurance take-up rates in Asia in 2017 with the current global premiums estimated to total $50 million.[7] The increase in cyber-attacks in 2017 in Asia over recent years means companies are more likely to have standalone cyber insurance than before, although with low sub-limits and more limited take-up of first party BI coverage when compared to other markets. Further insurance take-up is likely in the future for directors and officers (D&O) policies as changes in the business environment as such tight corporate governance and new regulations are introduced.

The expansion of the cyber insurance market is both necessary and inevitable. Scenarios such as the 'Bashe Attack' and the 'Shen Attack' will help insurers and policyholders to expand their view of cyber risks ahead of the next event and help them create new products, services and mitigation strategies that make businesses and communities more resilient. To achieve this continuing the collection and sharing of quality cyber-attack data is an important element that will enable technological and insurance solutions required for cyber risks that are constantly changing.

[6] Strictly speaking no affirmative standalone cyber cover or endorsement for Cargo is available. A notable exclusion in the Marine insurance industry is the Institute Cyber Attack Exclusion Clause (CL380). CL380 excludes insurance cover for risks occurring because of cyber-attacks. Within this scenario, marine policies are assumed to have a 50% exclusion rate to account for CL380.

[7] Williams 2016; Weinland 2017; OECD 2017

Introduction to the scenario

1. Introduction to the scenario

The Shen Attack scenario was created by the University of Cambridge Centre for Risk Studies (CCRS) as a fictionalised account of a catastrophic cyber event targeting the maritime industry. This is the second scenario in a series done in collaboration with Lloyd's and CyRiM. Much like the first scenario, 'Bashe attack: global infection by contagious malware',[8] this attack presents an unlikely and extreme, yet plausible, scenario that culminates in catastrophic economic and insurance losses.

World trade depends on the reliability and health of the international shipping industry. Almost every aspect of the shipping industry lends itself to cyber means. Global positioning satellites (GPS) allow ships to stay on course, reducing wait times. Marine Automatic Identification Systems (AIS) track and monitor ships, allowing suppliers and customers to know where their goods are and allowing for 'just in time' timelines to develop for fewer spoiled goods and wasted warehouse time. Electronic Chart Displays and Information Systems (ECDIS) and the associated digital nautical charts mean fewer crewmembers are needed, keeping costs down. These are only a few of the technologies that have allowed the maritime industry to grow and continue supporting world trade.

Today, international shipping is responsible for 90% of world trade by volume with over 55,000 cargo ships in active international trade providing, goods, services, and jobs worldwide. Over 1.5 million crew members are employed on international trading vessels.[9] The potential opening of Arctic Shipping Lanes heralds increasing connectivity between the Far East and Europe,[10] adding to the increase in global shipping connectivity.

Box 2: Shen attack

The Shen attack was named from Shèn 蜃, a shapeshifting sea monster or clam monster from Chinese mythology. The large-scale cyber-attack on ports scrambles records of container contents, causing widespread chaos and confusion.

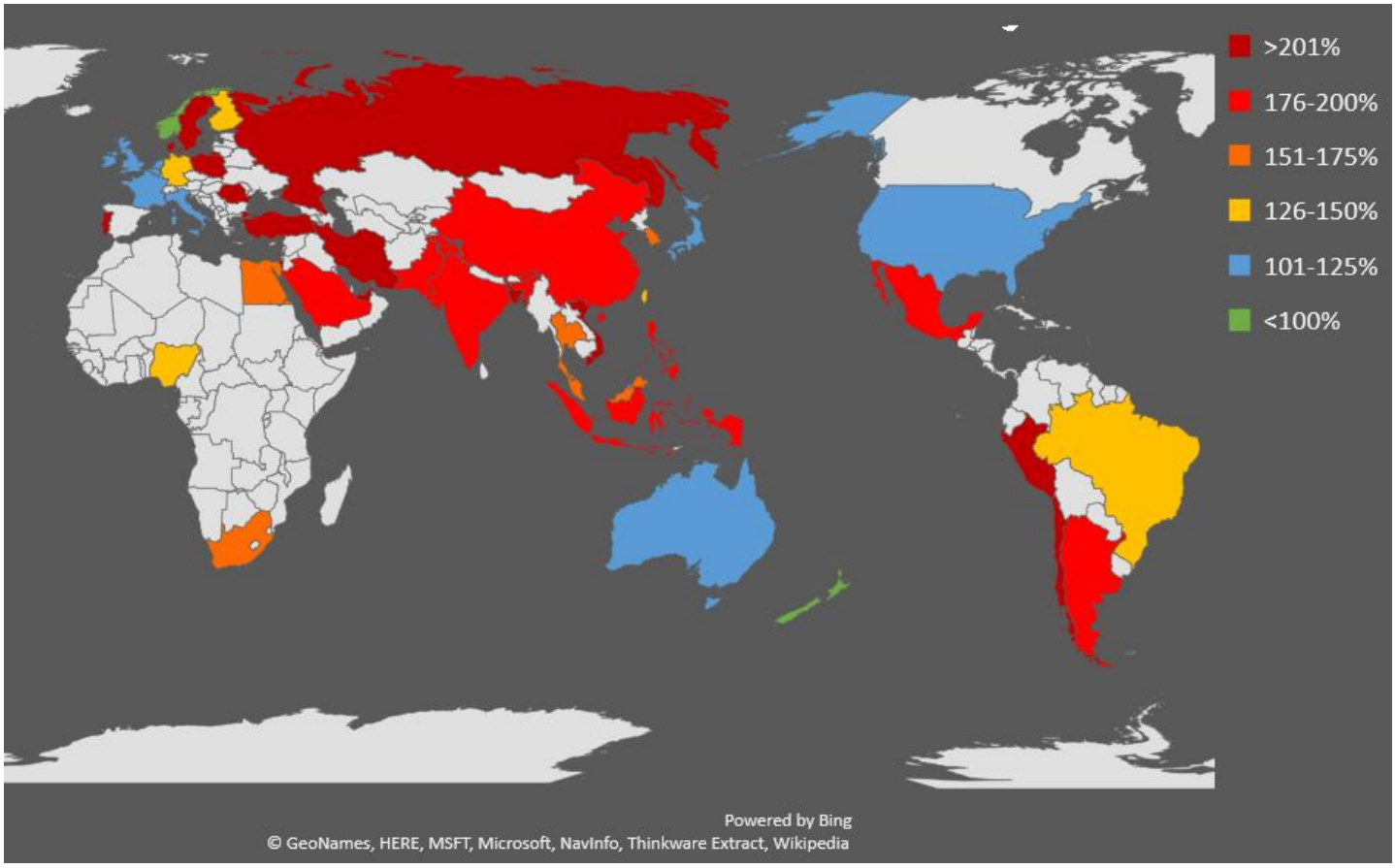
The scenario

The Shen[11] attack scenario depicts three scenario variants for impacts from a cyber-attack, which targets a popular ship management company with connections to ports across Asia. Ship management companies provide ship owners with crew to operate and maintain their vessels. They also offer a range of other services, including inspection, supervision, technical, business, and crew management.[12] Some ship management fleets are quite large, such as V.Group, the world's largest ship manager, which managers a fleet of 940 ships across 30 countries.[13]

The virus originates in a ship management company's cargo management software, corrupting the cargo manifests of the ships it manages. It then works its way laterally through links in the port management system supply chain to disrupt the first port of call for each of the infected ships. Once the corrupted manifests (cargo documents) are opened in destination ports, the virus spreads through the port's cargo management network.

[8] Cambridge Centre for Risk Studies, Lloyd's of London, and Nanyang Technological University 2019
[9] IMO 2019
[10] Murphy 2018
[11] Wikipedia 2017b
[12] SG Maritime 2018
[13] Lloyd's 2018

Figure 3: Increase in shipping connectivity from 2004-2018[14]



When the ships reach their destination port, the management services and logistics companies associated with each port authority are infected. The database records of contents of containers throughout the ports are scrambled, forcing port managers to shut the ports completely in order to manually sort through and identify cargo contents, spoiling perishable goods, and losing revenue from business interruption.

The results of three variants of this scenario are presented. All three scenario variants represent low-probability, high impact sets of consequences for this maritime attack that scrambles cargo content data and forces port closures. For the S1 variant, this attack directly affects ports in Japan, Malaysia, and Singapore. The S2 narrative and impacts extend the directly impacted ports to include ports in The Republic of Korea. The most extreme variant, X1, adds ports in China to the list of directly affected ports.

The attack cascades down the shipping supply chain, with downstream suppliers and third-party industries experiencing significant knock-on effects due to a loss in productivity from a delay in receiving goods.

Secondary and tertiary countries which have strong trade relationships with the directly affected countries suffer further due to this relationship and the inability of the directly affected ports to continue exports.

The Shen attack is not a prediction of events to come; it is a hypothetical account presented as a stress test to challenge industry understanding and preparedness for cyber-attacks. It highlights the importance of vigilance for all links in digital supply chains and third-party suppliers. Moreover, it is an exercise in understanding the holistic effects of a catastrophic malware event that affects an inherently complex industry and to raise awareness of the systemic threat of cyber to the maritime industry.

Section 2 details the events leading up to, during, and following the events of this extended attack for the S1 variant.

Section 3 gives an overview of the increased losses and ports affected in each variant of the scenario.

Section 4 and Section 5 outline the economic losses by sectors and regions. Section 6 explores the insured losses incurred from this scenario.

[14] UNCTADstat 2018

Shen attack scenario narrative

2. Shen attack scenario narrative

The complex logistics involved in the shipping industry has led to the rise of third-party ship management and management services companies. In-house services of crew management, contents management, maintenance, and dry docking, among others, can now be hosted by a third-party company, often separating the roles of ownership and management. This narrative aims to highlight the complexity of maritime digital supply chains and the potential for catastrophic losses if they are not adequately protected.

Phase 1: Accidental exposure

The global ship management company ClamStar Group[15] has subsidiaries in the Americas, Europe, Russia, and Asia. Each of these subsidiaries works independently of the others under the umbrella corporation of ClamStar. In a recent revamp to their Asian branch, the IT team unknowingly leaves a set of administrative passwords unprotected on their cloud server. This error is noticed by a small-time cybercriminal based in Southeast Asia while they are penetration testing various ship managers. The credentials give the cyber criminals access to the contents management system for all of ships managed by ClamStar Asia.

Phase 2: Taking advantage

The cyber criminals act fast to take advantage of the gap in security. They are eager to cause significant disruption in order to publicly claim the attack and make news headlines, establishing a formidable reputation. Their developers begin the work of designing and programming the virus they name 'Shen' from the Chinese mythological clam monster, mocking the targeted company. The virus is designed to scramble the data in the port management systems related to the cargo manifests of the ships managed by ClamStar Asia as well as any network the manifests are opened on.

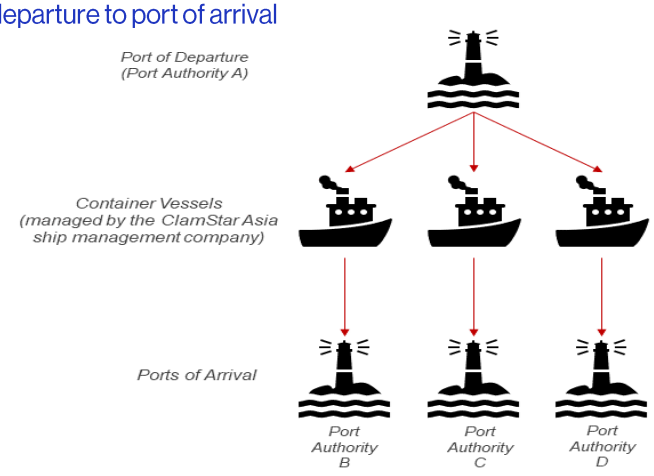
Phase 3: Patient zero

The ships managed by ClamStar Asia unknowingly become the first victims infected with the virus. Their cargo manifests are infected, and they become carriers of the chaotic virus. Short timelines, high crew turnover combined with the reduction of crew due to technology, and massive volumes of containers on each vessel means the crew are unaware that the original data of each container's contents have been contaminated. The manifests are sent to the first port of call and the ships disembark.

Phase 4: The spread

Cyber security vulnerabilities in the international shipping industry have been well documented and this occasion is no exception. Before disembarking, the ships send their manifests to their first port of call. Once opened at the receiving port, the virus spreads through the trusted port management network, scrambling the data in the databases. It is unknown which ships have scrambled content records or are now carriers of the virus. The primary management services and logistics companies at each port are also infected on receipt of the cargo manifests

Figure 4: How the Shen scenario unfolds, from port of departure to port of arrival



[15] ClamStar Group is a hypothetical ship management company modelled after current examples.

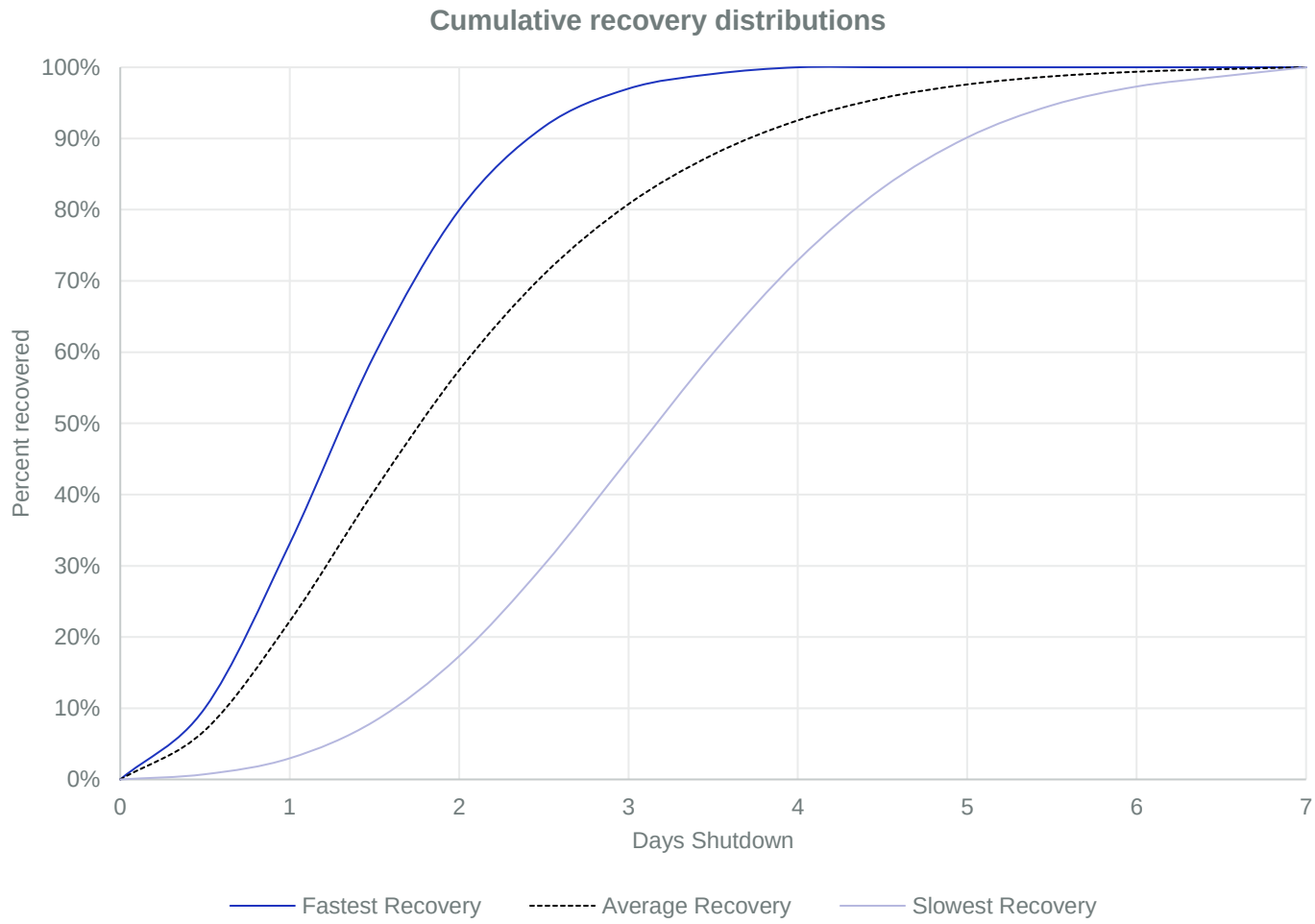
Phase 5: Containment

Affected ports are forced to shut down to prevent the spread of the virus to other ports and ships around the world and to correctly identify the contents of the containers. The number of corrupted manifests temporarily halts port activities and requires each container to be verified in person. Port and ship management systems are taken offline provisionally. Ports are closed for several days until the damage is evaluated and the cargo details are manually verified.

The length of closure for each port is influenced by number of containers at the port and the efficiency with which they can examine container contents and ship software. The resilience plans of infected ports allow for the swift addition of extra staff into the ports to address the chaos of scrambled container data, which puts the ports at a greater risk of theft during this period. Management must take on the role of coordinating contracted and non-contracted workers and emote a sense of organisation and confidence. It is unknown how many containers have been mislabelled and which ships carried the malware into port, therefore all containers in the ports of closure must be manually searched and their contents logged into a new system along with a full software scan onboard all docked ships. Operational staff revert to pen and paper logging, prolonging the closure period.

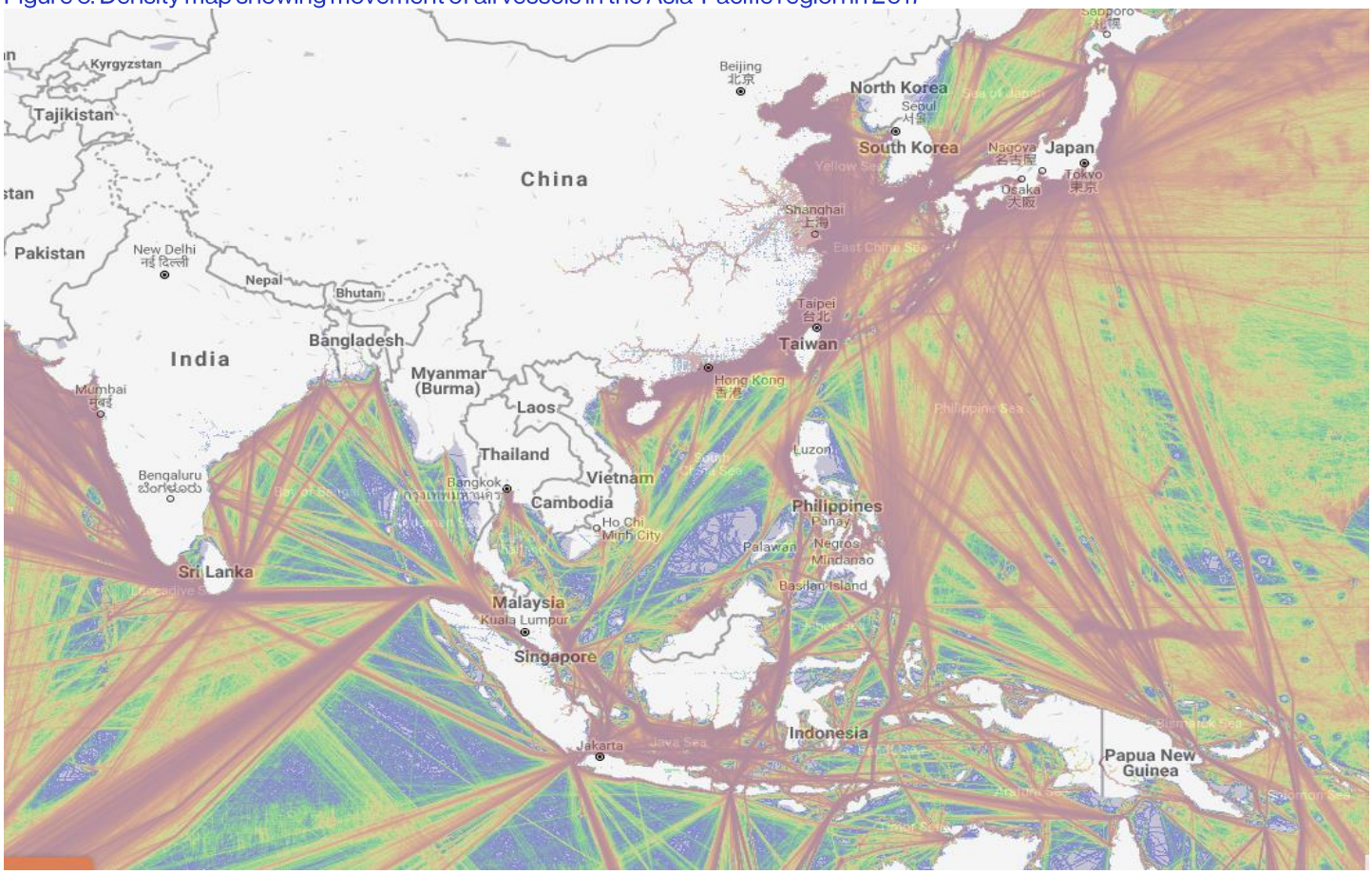
Figure 5 shows the cumulative recovery distribution curves by fastest and slowest recovery for the ports affected in the attack. It shows the number of days until the affected ports are fully recovered from the attack in terms of being able to return to full capacity. For example, the average recovery time in this scenario for a port to have 80% of its operations return to full functionality is 3 days.

Figure 5: Port recovery curves showing the time until each country is fully recovered from the attack in each scenario variant



Global shipping networks are disrupted as the goods to be delivered to the affected countries need to be rerouted if possible, and the goods coming from the affected countries are left stranded in the port until they can be identified. Some shipments can be redirected to nearby ports in neighbouring countries. However, millions of Twenty-foot equivalent units (TEUs) of perishable good are lost in the process of container identification.

Figure 6: Density map showing movement of all vessels in the Asia-Pacific region in 2017[16]



Phase 6: Attribution

One day after the ports have been forced to shut down container terminal operations, the news media begins reporting on the widespread economic and logistical damage the attack is causing. The official port authority websites of the primary targets are hacked by the cybercriminals and defaced with their logo as they proudly take responsibility for the attack. Reporters pick up on this and they become a household name across the world within the week.

[16] Screen grab of Marine Traffic 2019

Scenario variants

3. Scenario variants

The Shen attack scenario presents three variants of the narrative. This narrative is a hypothetical set of events that scales up in economic losses and impact with each variant. The losses for each variant are highly dependent on the countries directly affected and their respective maritime profiles and global supply chains. When considering the scenario's impact on industry, it is important to note that these attacks can be replicated on any set of ports in the world that share a common network. Changing the identity of the countries will directly affect the total losses. It should be highlighted that in our X1 scenario we will be affecting 9 of the top 10 ports by TEU in the world for 2018, which contributes significantly to the catastrophic economic losses.[17]

Overview

In each variant, a different ship management software is targeted with increasing permeation in the market. The number of countries with ports impacted therefore increases with the popularity of the software which houses the vulnerability.

The losses scale up with each additional country impacted in each scenario variant, ranging from $40.8 billion dollars of economic damages in S1 to $109.8 billion dollars in X1 where five countries are directly affected.

The total economic loss in X1 (approximately $110 billion) is just under 1% of the value of global seaborne trade, valued at $12 trillion in 2017.[18]

Table 3: Countries affected in each scenario variant

Scenario variant	Countries with ports directly affected	Number of ports affected	Total economics losses ($bn)
S1	Japan, Malaysia, Singapore	6	$40.8
S2	Japan, Malaysia, Singapore, The Republic of Korea	9	$55.9
X1	Japan, Malaysia, Singapore, The Republic of Korea, China	15	$109.8

[17] World Shipping Council n.d.

[18] Statista 2018

Table 4: The TEU affected within each variant

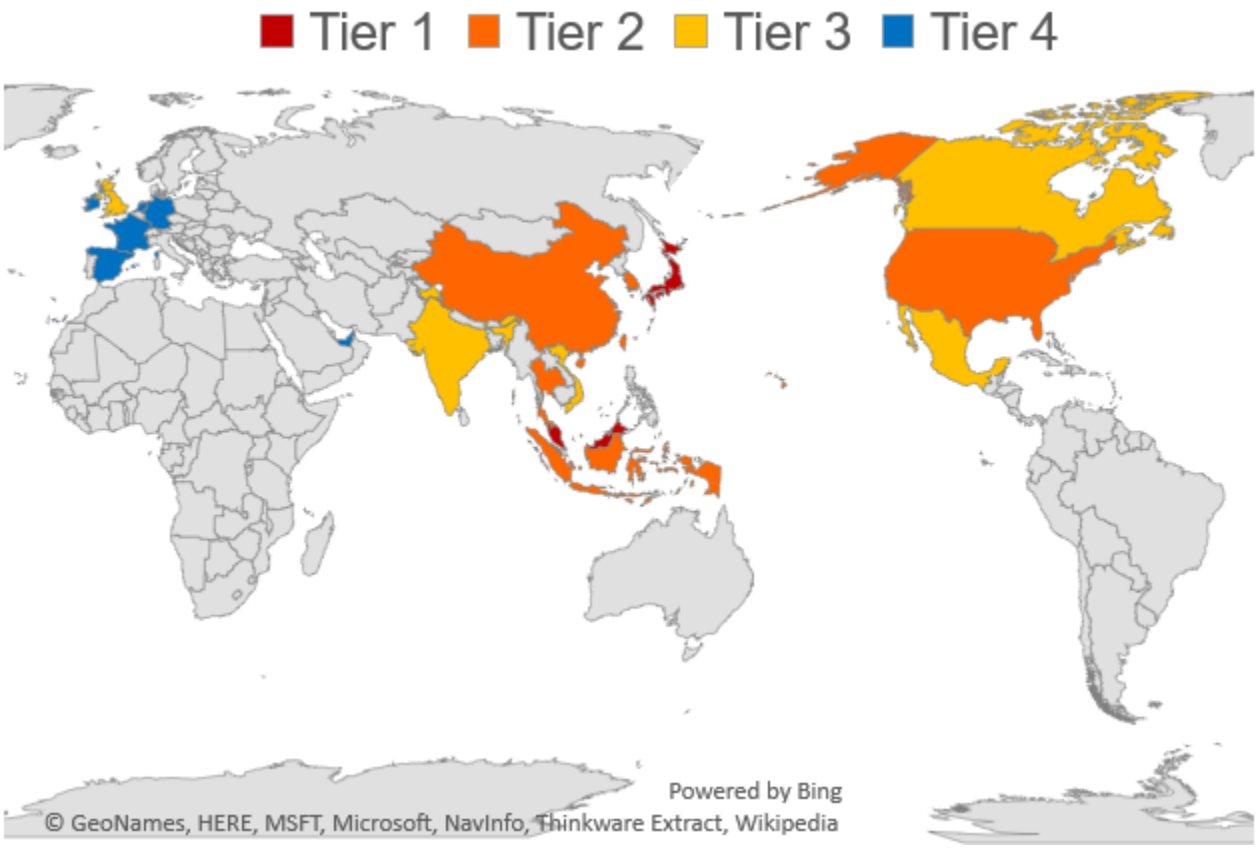
Country	Ports affected	Affected TEUs[19]
S1	6	1,156,232
S2	9	1,427,783
X1	15	3,688,879

S1 variant

The S1 variant is presented as the most likely of the three scenarios due to the scale of losses rather than due to the countries impacted. The countries directly affected in the S1 scenario are Japan, and Malaysia, and Singapore. Even with a constricted view of their maritime supply chain, the effects are felt around the world.

Figure 7 shows the level, or tier, at which various additional countries are affected down the supply chain. Tier 1 shows the directly impacted countries in this scenario variant: (Japan, Malaysia, Singapore. The second tier (orange) displays the top 5 trading partners of each of the affected countries, this includes the US and China. The tier 3 countries, such as Canada, Mexico, and India, are the top 5 affected through their maritime trading partnership with tier 2 countries, and so on.

Figure 7: S1 scenario variant global impacts.



Countries impacted are colour-coded to match the tier in the supply chain at which they are first impacted.

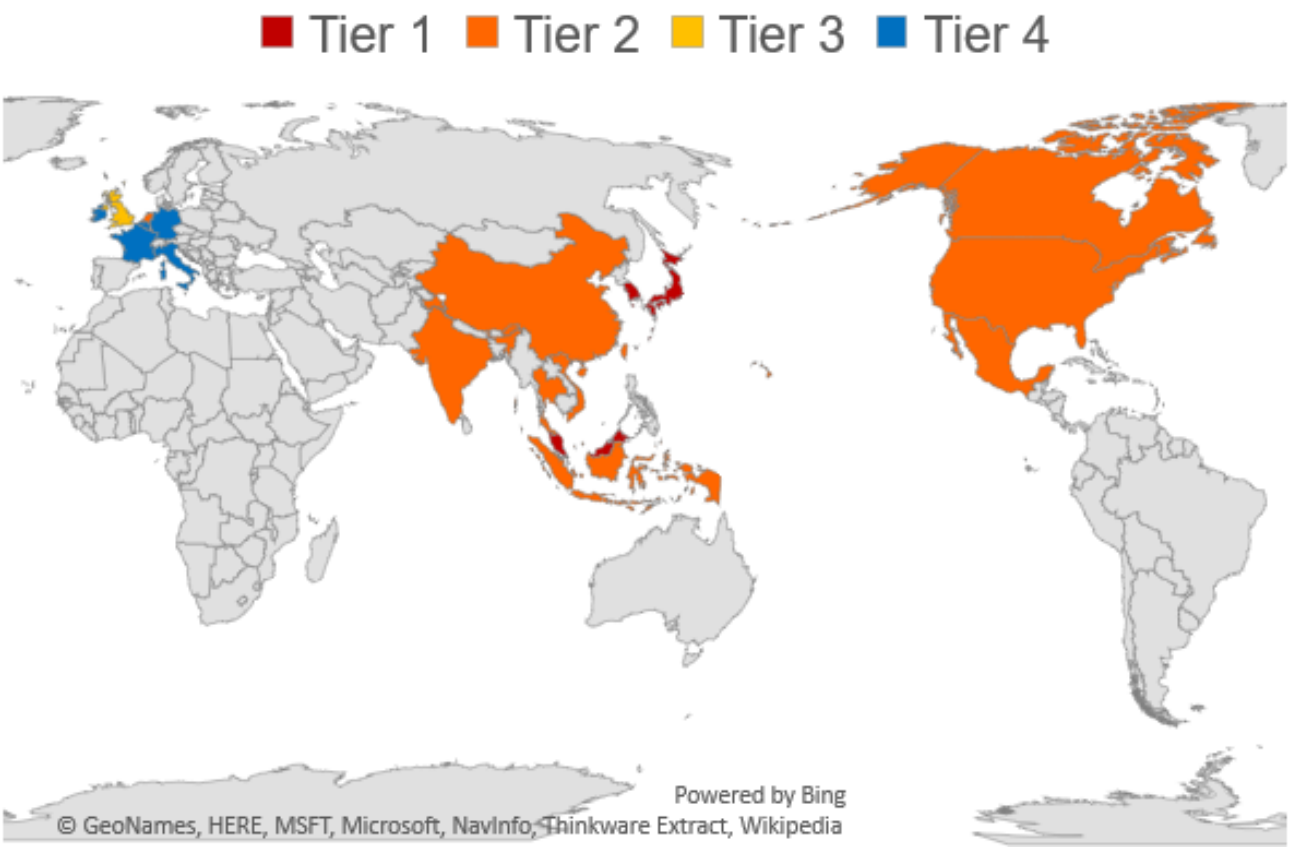
[19] TEUs for Ports listed in (Lloyd's List 2017)

S2 variant

The S2 variant extends the S1 impacted countries to include The Republic of Korea making the tier 1 affected countries Japan, Malaysia, Singapore and The Republic of Korea. The addition of The Republic of Korea to the narrative widens the number of countries affected even within the restricted view of the scenario losses.

Figure 8 shows the level, or tier, at which various additional countries are affected down the supply chain. Tier 1 shows the directly impacted countries in this scenario variant (Japan, Malaysia, Singapore, The Republic of Korea). The US, Canada, Mexico, China, India, and Indonesia are subsequently impacted the next level down the supply chain (tier 2) due to their close maritime trading partnerships with the tier 1 countries, and the tier 3 countries, such as the UK, are affected through their maritime trading partnership with tier 2 countries, and so on.

Figure 8: S2 scenario variant global impact



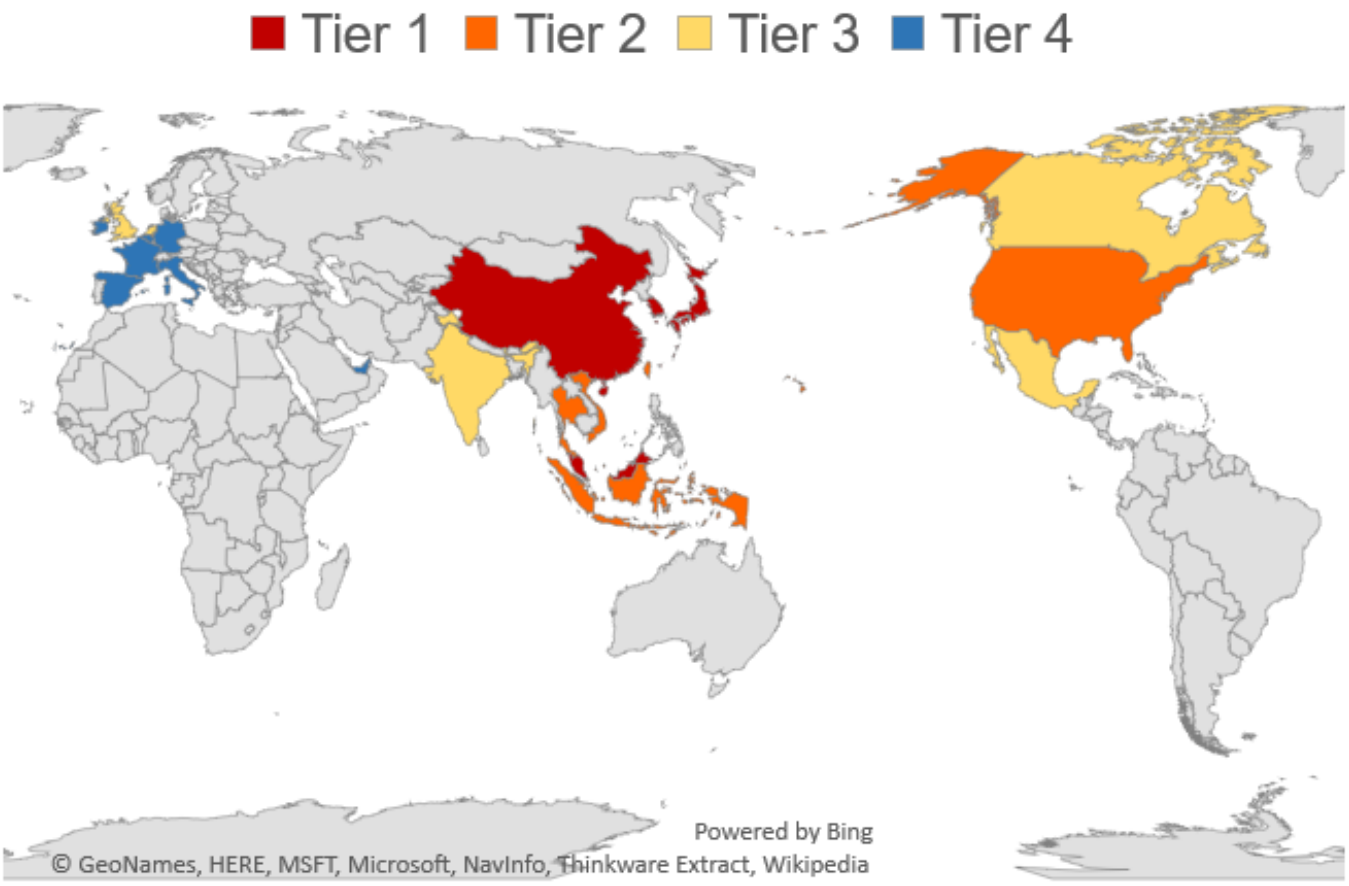
Countries impacted are colour-coded to match the tier in the supply chain at which they are first impacted.

X1 variant

The X1 variant is the most extreme variant, affecting over 35% of the global TEU throughput and increases both the losses as well as the reach of the scenario. The addition of Chinese ports to the narrative created this large increase in impact.

Figure 9 shows the level, or tier, at which various additional countries are affected down the supply chain. Tier 1 shows the directly impacted countries in this scenario variant (Japan, Malaysia, Singapore, The Republic of Korea, China). The US and Indonesia are subsequently impacted the next level down the supply chain (tier 2) due to their close maritime trading partnerships with the tier 1 countries, and the tier 3 countries, such as the UK, India, Canada, and Mexico, are affected through their maritime trading partnership with tier 2 countries, and so on.

Figure 9: X1 scenario variant global impact



Countries impacted are colour-coded to match the tier in the supply chain at which they are first impacted.

Key aspects contributing to losses

The number of ports within a country

A cyber-attack to an international port and key shipping routes inevitably comes with a range of detrimental consequences for many sectors. Though ports are similar in many fundamental ways, such as operations and personnel, they can differ widely in terms of cargo types, freight statistics, ship and cargo monitoring, operational technologies, and geographical considerations. For some of the countries affected by the Shen attack, the effects will ripple through the supply chain to hundreds of minor ports in the country.

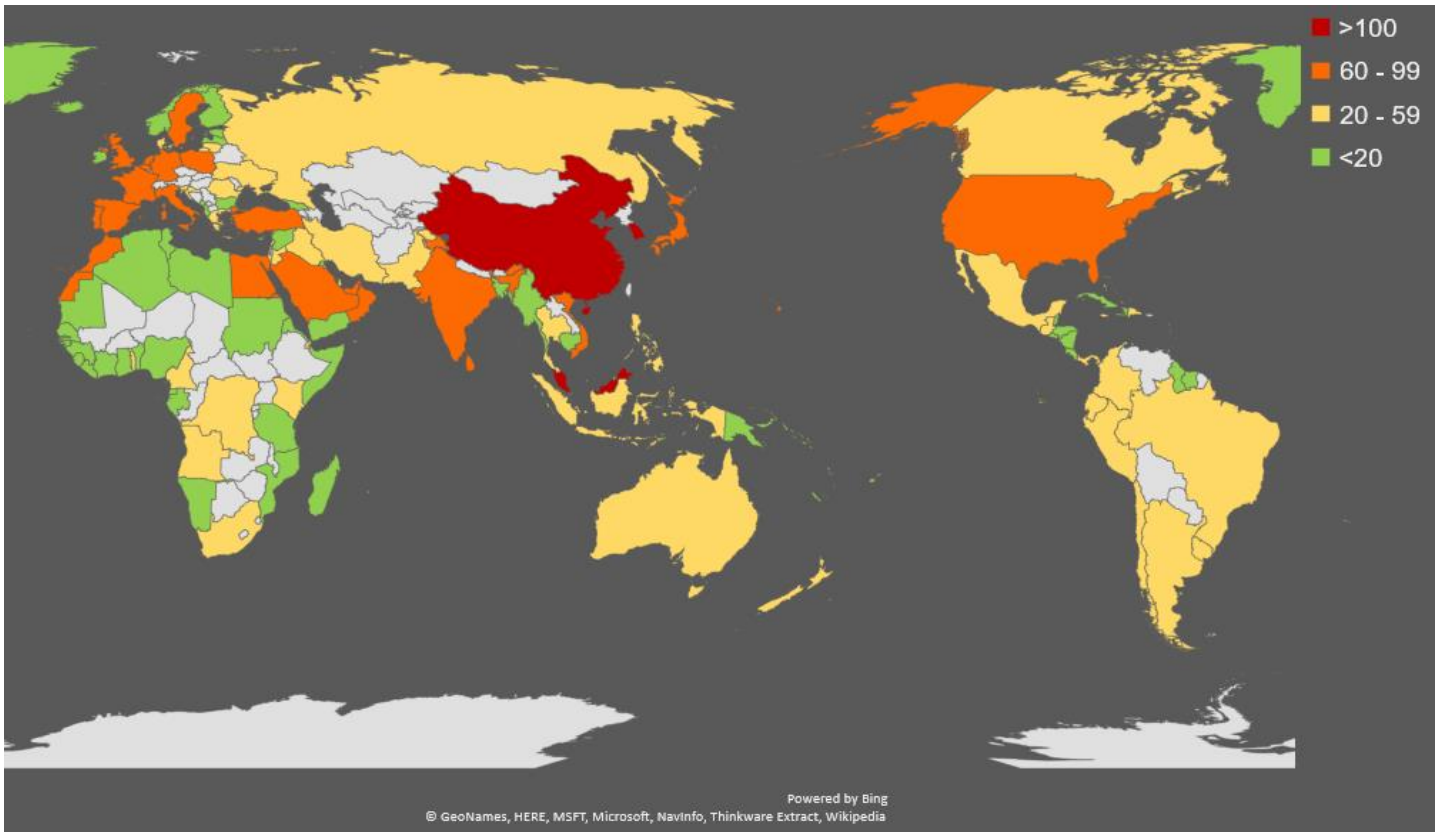
Port efficiency

Port efficiency incorporates information on business subscription, the size of vessels that can be accommodated within a port, and the technical efficiency with which cargo is received and released from ports. A metric for understanding a port's efficiency is the Varying Return to Scale or (VRS) score[20] for container throughput. The better the efficiency of a port, the less downtime they will experience in an event such as this. TEU throughput is also a standard measure of productivity for a port.[21]

Port connectivity

The interdependent and complex nature of maritime supply chains is well documented. Figure 10 shows the annual liner shipping connectivity index (LSCI) for each country. The LSCI considers the number of companies that deploy container ships on services to and from a country's ports combined with other measurements to capture the country's level of integration into the liner shipping network and trade facilitation.[22] As shown in Figure 10, the top three most connected countries in order are China, Singapore, and The Republic of Korea. In the event of a port attack, suppliers to, and those reliant on, these countries will be particularly hard hit.

Figure 10: Liner shipping connectivity index[23]



[20] "Efficiency of World Ports in Container and Bulk Cargo (Oil, Coal, Ores and Grain)" 2012
[21] UNCTAD 2017
[22] Transport Geography 2017
[23] UNCTADstat 2018

Surrounding area

The GDP of neighbouring countries may impact the cargo throughput of the affected ports because the cargo throughput of geographically near ports are dependent on each other.[24] This is in part due to transhipments, where goods are shipped to intermediate destinations before reaching their final port. An increased ability to handle transhipping operations at neighbouring ports combined with an increase in cargo throughput at the destination ports leads to this interdependency, making GDP an important determinant of container throughput.

In the event of a severe cyber-attack, ships will be rerouted to nearby ports where possible but, for some countries surrounded by countries with a lower GDP, this will have limited efficiency and possibly slow recovery. China, for example, is surrounded by neighbours with lower GDPs, so it may benefit more from focusing its efforts on returning to normal operations and rerouting vessels to other ports within the country rather than relying on capacity at nearby ports in neighbouring countries.

Table 5: GDP of countries directly affected and neighbouring countries[25]

Country	2017 GDP ($ millions)
China	12,237,700
Japan	4,872,136
The Republic of Korea	1,530,750
Australia	1,323,421
Indonesia	1,015,539
Hong Kong Special Administrative Region of the People's Republic of China	341,449
Singapore	323,907
Malaysia	314,710
Philippines	313,595
Vietnam	223,779

[24] Wang 2014
[25] The World Bank 2017

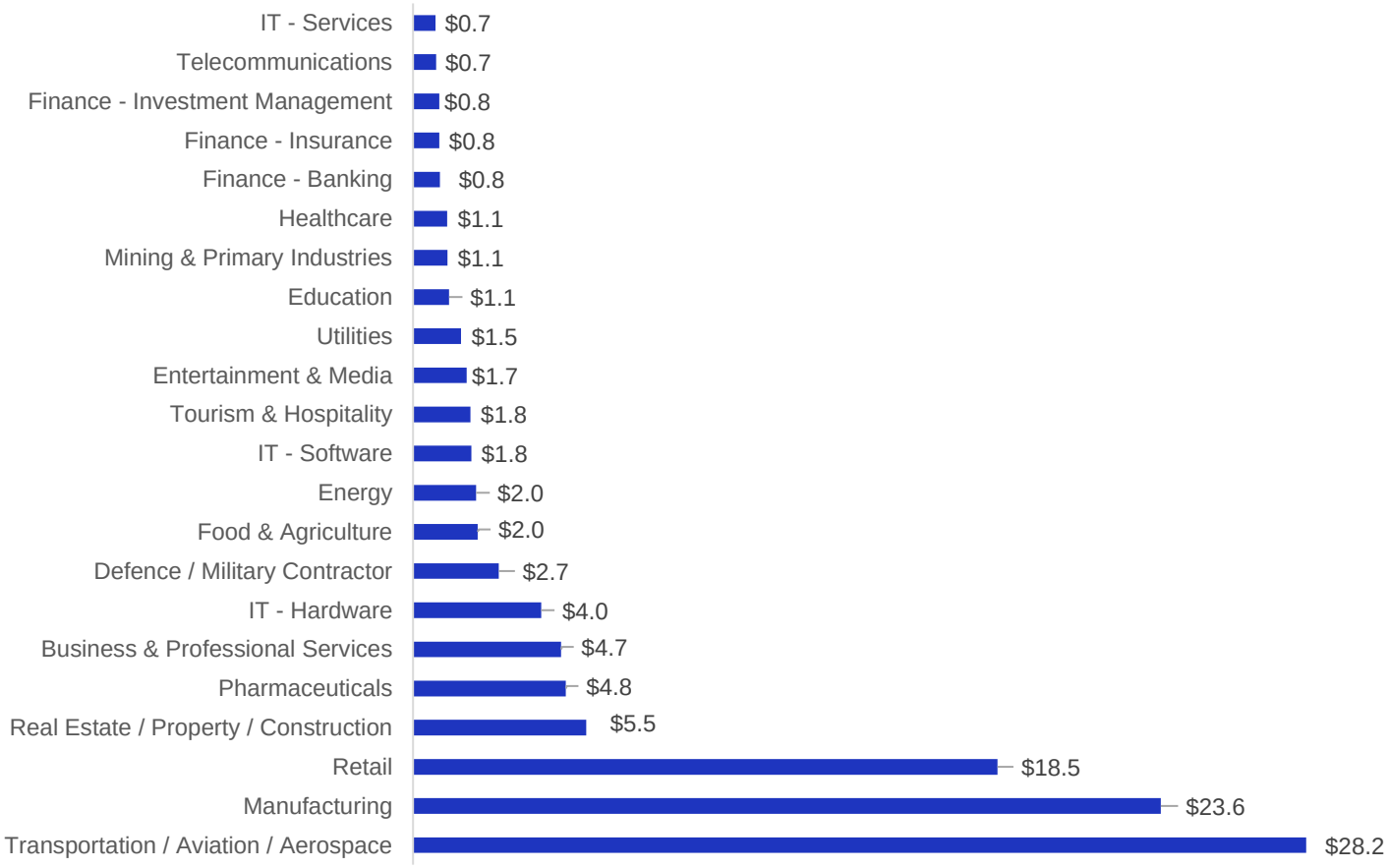
Sectorial impacts

4. Sectoral impacts

Though the associated port authority for a port shoulders the worst of the economic impacts, a port is a commercial facility for maritime transport and is home to several commercial stakeholders who supply and operate in a range of business activities and marketplaces. This section provides a qualitative analysis of port closures to these stakeholders and industries that are affected as a consequence of this attack that contribute to the losses seen in Figure 11.

The following sectoral analysis has been conducted to trace the impact on a port through to its commercial stakeholders. Sectoral losses are calculated using the OECD input-output tables for the five directly affected countries.[26] Sector names were translated into CCRS sector names along both axes and then the sectors were ordered according to their dependency on the Transportation sector.

Figure 11: Global sectoral losses from port closures by sector ($billions) for variant X1 (all five directly affected countries)



.

[26] OECD 2015

Global primary sectoral effects

Transportation

Because the data scrambler attacks the container database management systems, container ships are the most impacted vessels. However, other vessels will suffer delays and possible infection as a result, including oil tankers, bulk carriers, and general cargo ships.

Due to severe congestion and the reprioritisation of workers to focus on the attack, ports would be unable to receive cruise ships, which would be forced to either anchor outside the port, extend their sailing period, or be diverted to another port that could accommodate them. This impacts the tourism industry as passengers do not disembark at the intended destination, resulting in less time and money spent in the local economy. Some cruise liners offer passenger compensation.

Heavy-haul trucks used for transporting goods to and from the container storage units and directly from the docked ships are stranded in long queues outside the port in both directions, creating an unmoving line of heavy-duty trucks on the main roads.[27] Truckers are unable to pick up their cargo because operators cannot determine what cargo should go to which haulier.

This has severe knock-on effects for general commuter traffic; commuters find themselves unable to use key roads to get to work, leading to a decline in production at geographically neighbouring industries, including petroleum refineries, restaurants, chemical manufacturing plants, nearby shipping terminals, shipbuilders, power utilities, passenger transport, access to customs checks within the port area, recreational activities near beaches, and deterring people from booking into any hotels near the port.

For more geographically isolated nations this temporary disruption to the Transportation sector causes panic amongst consumers as grocery store shelves are empty of key goods, in some cases leading to store closures and stockpiling. Retailers are forced to leverage alternative supply routes, such as air freight, to import reserves from other suppliers and countries where necessary.

Because of the diversity within the transportation sector, which encompasses maritime, road, rail, and air traffic for commercial and non-commercial use, the effects of the Shen attack are most keenly felt in this sector.

Table 6 shows the percentage of output from the Transportation sector for each country. Each country column (summed vertically) equals 100%. For example, 44% of the output from the Transportation sector in Singapore goes back into the Transportation sector, 11% of the output from Transportation goes to Manufacturing, and so on. This is based on data from OECD input-output tables.[28] Though Business & Professional Services is only in the top 5 for The Republic of Korea and China, the losses are significant because of the heavy losses felt in China, driving up the total impact.

Table 6: Percentage of output from the Transportation sector[29]

	Japan	Malaysia	Singapore	South Korea	China
Transportation / Aviation / Aerospace	23.70%	31.00%	44.80%	29.50%	20.50%
Manufacturing	24.40%	14.90%	11.60%	21.30%	24.40%
Retail	17.90%	16.00%	10.90%	16.90%	18.10%
Pharmaceuticals	4.10%	3.30%	6.30%	4.20%	4.50%
IT - Hardware	1.30%	7.80%	5.80%	3.00%	3.40%

[27] Box 3 *"Calais Strike Clogs UK Roads"*: News24 2015

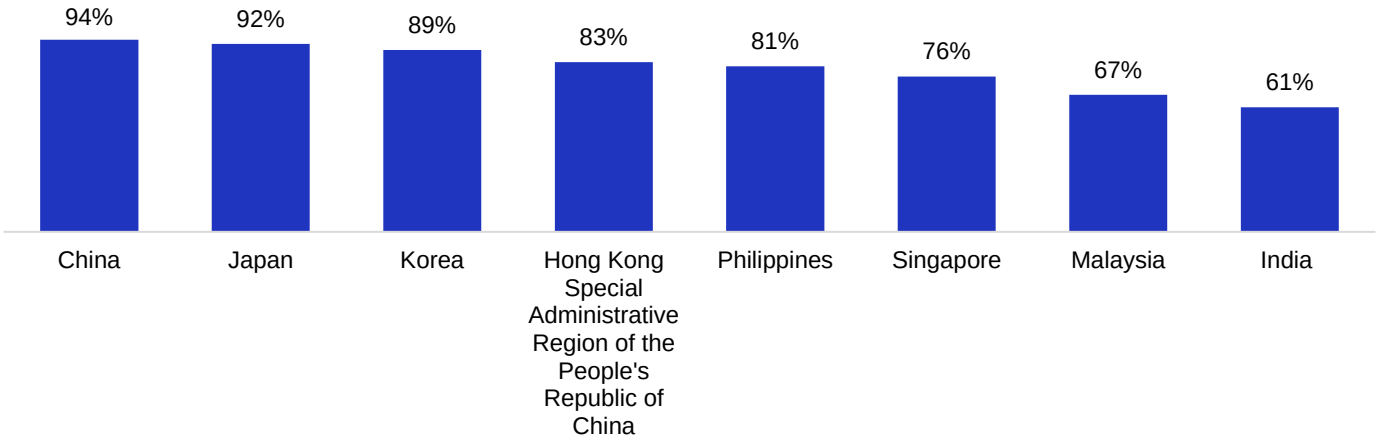
28 OECD 2015

29 OECD 2015

Business & Professional Services	3.00%	2.60%	4.70%	4.70%	4.90%
Real Estate / Property / Construction	5.90%	2.20%	3.30%	3.70%	6.10%
Defence / Military Contractor	2.40%	3.10%	3.20%	2.60%	2.20%
IT - Software	0.60%	2.60%	2.90%	1.50%	1.70%
Entertainment & Media	3.10%	1.20%	1.40%	2.20%	1.00%
IT - Services	0.80%	0.60%	1.00%	1.00%	0.50%
Utilities	2.80%	0.90%	0.70%	1.80%	1.10%
Tourism & Hospitality	3.00%	0.80%	0.60%	0.70%	1.90%
Finance - Banking	0.50%	3.60%	0.60%	0.80%	0.30%
Finance - Insurance	0.50%	3.40%	0.60%	0.80%	0.30%
Finance - Investment Management	0.50%	3.40%	0.60%	0.80%	0.30%
Education	0.80%	0.80%	0.40%	1.70%	1.10%
Telecommunications	1.20%	1.70%	0.40%	0.70%	0.30%
Healthcare	2.00%	0.40%	0.30%	1.20%	0.90%
Food & Agriculture	1.30%	2.30%	0.00%	0.60%	2.70%
Energy	0.00%	5.80%	0.00%	0.10%	2.40%
Mining & Primary Industries	0.20%	1.20%	0.00%	0.20%	1.70%

Manufacturing

Figure 12: % of manufactured goods as a percentage of total country maritime exports[30]



Car manufacturers suffer heavy delays as the congestion impacts shipping terminals whose primary function is to roll new automobiles directly onto trucks from the docked ships. Workers from these terminals, where cargo is easily identifiable, are reassigned to conduct visual inspections on affected storage areas for the purposes of cataloguing and quality control. This causes ripple effects throughout the automobile supply chain, including a delay in cars having parts fitted and being distributed to dealerships. Where possible, ships are rerouted, but for many geographically isolated ports, or ports which lack neighbouring ports with the necessary capacity or functionality to accommodate new automobiles, this is not a manageable solution, and ships remain at the affected port until it reopens.

Production at chemical manufacturers, petroleum refineries, and related engineering activities are impacted due to traffic congestion around the port. Further down the supply chain, even geographically far-flung manufacturers struggle as equipment, products, and parts they were expecting fail to arrive on schedule, leading to a decline in their output and a production slowdown.

Retail

The 'cold chain', which is the temperature-controlled supply chain, is a crucial part of transporting food items and perishable goods distributed by retailers to consumers. Refrigerated containers, otherwise referred to as reefers, are containers with temperature control and data logging functionality. Reefers are used in the maritime transportation for goods in the cold chain and for quality assurance. This cold chain requires a constant data log of temperature over time.

In the Shen attack, the cold chain is broken as the data of containers is scrambled, resulting in a gap in the temperature log. Regardless of the robustness of the cold chain, without any data to prove the bounds of the temperature range for quality assurance purposes, the contents are considered compromised. Many reefers may rely on Remote Container Management (RCM) devices, which are connected devices that relay tracking information of the container contents to a centralised database or port management system.

However, in the event of the Shen cyber-attack, the database and port management system itself is compromised. Some containers may be easier to assess in person if they have RCM devices with digital displays for workers to verify the temperature logs. However, in all instances, congestion at container terminals will lead to perishable goods remaining in storage past their expiry dates.

Ships that were moving into port at the time the virus is released are rerouted to nearby ports causing congestion at uninfected ports. Goods loaded onto trucks also suffer severely as a result of long waits in trucking queues. Emphasis is placed on identifying all refrigerated containers as quickly as possible to prioritise moving those goods and to make sure the refrigeration has not been compromised. For the largest ports serving the largest population areas, a decline in available food items results in empty shelves in grocery stores as certain items are unavailable and a public outcry from consumers unable to find the items they are looking for, especially meat, fish, fruit, vegetables, and dairy products, with prolonged shortages driving up the price.[31]

Non-food-related goods are similarly affected. Automobiles, automobile parts, machinery, and applications are unable to reach wholesalers and distributors on time, leading to shortages on the consumer end. This affects a wide range of goods, from phones and appliances to apparel and household goods like cleaning supplies.

[30] UNCTAD 2017

[31] CNN 2011

Real Estate, Property, and Construction

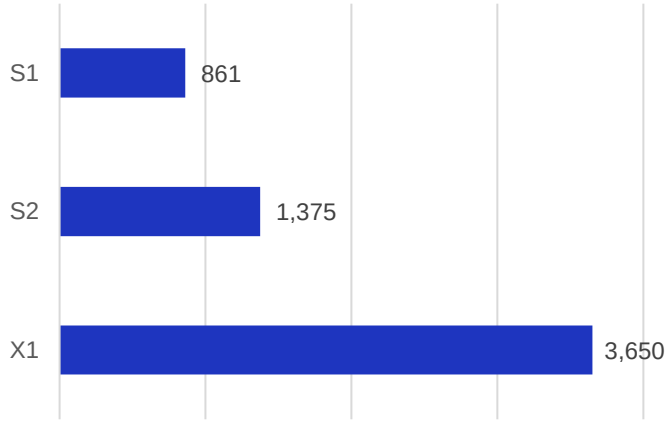
On average, the Real Estate sector in the countries directly affected by the Shen attack relies on 3% of economic input from the Transportation sector, and outputs 6% to the Transportation sector. This is primarily the Construction portion of the Real Estate sector, which requires transportation for construction materials to and from building sites.

Once the ports are affected by Shen and the first-level sector, Transportation, suffers, the Real Estate sector will lose some of the input from Transportation it requires for its own services, in turn compromising the output it can return to the Transportation sector. This positive feedback loop compounds the damages and delays recovery.

The Real Estate sector in each country relies primarily on input from Manufacturing for its construction activities and, less so, on the Finance sector. Because of these sectoral inter-dependencies, once the ports are affected and Manufacturing is impacted, Real Estate / Property / Construction will suffer losses as a result, with effects flowing from multiple sectors to multiple sectors. For China and The Republic of Korea, the two directly affected countries where Real Estate is the most dependent on Manufacturing to supply machinery and construction materials, the effects may be catastrophic. The other directly affected countries may have similar effects in the Finance and Mining and Primary Industries sectors as well, depending on the country's economy. Business and professional services

Because of the ubiquity and range of business and professional services, this sector suffers significant losses. CCRS modelling uses OECD input-output tables at the country and sectoral level. The cost is great for onsite business professionals because work grinds to a halt as they are unable to perform their duties or even reach their physical places of work due to the collapse in the transportation network and resulting congestion. In addition, software that companies rely on for scheduling, data management, and daily operations are exposed and require other business professionals to evaluate and repair. Time is invested in reverting to data backups, conducting forensics to isolate and fix the source of the intrusion, and repairing gaps in data records.

Figure 13: Direct economic impact to the Business & Professional Services sector in each directly affected country ($ million)



The Business sector includes occupations that require special training or professional licences such as doctors, lawyers, architects, accountants, and engineers. A need for management consulting, cyber awareness and defensive training, and legal advice will spike in the recovery period of the cyber-attack. Marine engineers and naval architects may be brought in to assess any physical damages that may have resulted from changes in the routine of vessels and conduct repairs. Since the Shen attack scrambles sensitive data in the database management systems, accountants are engaged to comb through the damaged database and see what can be pieced back together from available backups and records, spending hours reconciling retrieved records with available data from suppliers and backups.

Pharmaceuticals

As the scrambling virus takes effect, the shipping companies lose track of cargo intended for critical uses. Medical equipment and pharmaceuticals are difficult to locate for the period of the outage. For medicines that require a temperature-controlled environment, the situation becomes particularly dire as workers struggle to know which containers require refrigeration and focused monitoring to ensure an unbroken cold chain.

Though Remote Container Management (RCM) devices may make it faster for workers to verify container contents and the level of container compromise if each RCM device has a digital display, the data sent to the port management system is no longer trustworthy. This compromises the quality management systems in place to offer assurances to business partners and consumers about the cleanliness and quality of their products. A common temperature range for pharmaceuticals is 2 to 8°C (36 to 46 °F),[32] but the specific temperature depends on the tolerance of the individual product being shipped.

Necessary air quality levels (carbon dioxide, oxygen, and humidity) further complicate these systems. Once the cargo is located and the process begun to contain and scrub the virus from the systems, the inspection process for pharmaceuticals is particularly lengthy, as each container must be evaluated with care to determine damages.[33]

Box 4: Merck unable to meet demand for HPV vaccine

After NotPetya hit in 2017, Merck suffered the biggest losses of a single company, close to $1 billion. This was in part due to a reduction in sales due to an inability to meet demand for Gardasil, the HPV vaccine. Merck had to borrow $240 million worth of Gardasil doses from the CDC's stockpile.

Global aggregate effects

Trade and productivity

Containerisation offers great convenience in easily transferring goods between different modes of transport, allowing door-to-door transportation for goods exported from all over the world, creating a flourishing trade. Global sourcing and interconnectivity, illustrated by the Liner Shipping Connectivity Index (LSCI), has further contributed to the integration of ports into supply chains.[34] A port shutdown would block exports for other markets and cause disruption of production up and down the supply chain and across country borders.

The effect on trade and production is unavoidable. Production is rescheduled and personnel must work overtime or extra shifts to recapture lost production after the port is opened. These actions are taken by companies throughout the supply chain, not just at the ports. Downstream production is constrained by material and equipment shortages. As exports are restricted, demand increases for inputs for production, leading to rising costs. This creates a chain reaction of losses and decreases in production activity from first-round suppliers who are unable to afford certain goods.[35]

In some cases, ships can be rerouted to other ports. Petroleum products, which require specialised facilities, may be rerouted to undergo refining and processing at other ports, though this requires ports to have the necessary pipelines and transportation modes/routes established.

For ports adjacent to or in large metropolitan areas, sections of the economy and community in the immediate vicinity rely on the work generated by the port operations. With the port shutdown and heavy traffic congestion gridlocking arterial roads, urban areas suffer production slowdowns as workers struggle to make their way to offices and are unable to perform everyday tasks that rely on a constant flow of output from the port. Shift workers, occasional workers, contractors, and part-time workers who are paid hourly suffer losses of income as the port is unable to employ them in their routine capacity for the duration of the shutdown. If investments and expansion plans are reviewed as a result of the cyber-attack, opportunities for employment may be squashed and there may be prolonged effects on infrastructure development.

[32] Outsourcing Pharma 2017

[33] Box *"Merck Unable to Meet Demand for HPV Vaccine"*: The Security Ledger 2017

[34] Loh and Thai 2015

[35] Rose and Wei 2013

Information technology

There is an increased demand in consultants and software experts as port authorities and firms attempt to determine if Shen can be reverse engineered to retrieve the scrambled data. Port authorities rely heavily on internal IT support staff for their day-to-day operational needs. In the event of a cyber-attack, the support staff will be inundated with calls from individuals within the organisation to identify the problem. Staff will be desperate to remedy the situation so they can continue work, leading to considerable strain on IT support services. When the port authorities realise that the data cannot be retrieved, they resort to bringing in contractors, both manual labourers and IT experts, to help bring the port back online as not all ports have the internal resources to cope with the scale of the situation.

Some of the information stored within the port systems' database infrastructure is sensitive and unable to be salvaged, exposing the port to fines under data privacy regulations. Data that is important for the management of the ports is lost, such as payroll numbers, which puts further strain on the organisations to resolve their internal databases. This also constrains their ability to bring in consultants and contractors as they are unable to access their finances.

Scrutiny is placed on software providers and database management systems as port management companies question their robustness and resilience, leading to a decrease in the revenue of database providers as new contracts are not taken out and existing contracts are not extended.

Finance

As confidence in maritime trade services declines, stock prices in transport services begin to fall. This impacts a variety of investment funds as fund managers look to offload their investments in some areas of the maritime industry. Ports investing in new container terminals that rely heavily on automation are especially at risk of losing investors, compromising their further development.

Some enterprises are forced to sell shares to obtain the extra funds necessary, as they do not have sufficient emergency fund supply to investigate and restore services. Premier companies struggle to obtain cash through stock offerings when share prices are down as the same number of shares sold at a lower price will raise less money. Depressed stock prices increase the cost of borrowing, because the banks offering loans take a company's share price into account when deciding whether to extend credit and at what interest rate. Many businesses, especially young businesses in industries with high research and development costs, cannot survive without access to cheap capital.

Goods are no longer being delivered and, as commercial invoices are generally issued on the receipt of goods, available cash flow plummets, in turn impacting businesses, particularly smaller and medium sized enterprises, which are not as resilient to financial shocks. This leads enterprises to either go out of business or seek emergency loans to cover their overheads and fund existing projects until invoices are met, which are difficult to obtain and have high interest rates. As more money is borrowed at higher interest rates, inflation around the globe will rise, impacting consumers.

Long-term effects

The port closures lead to the permanent loss of business in some areas as port businesses opt for new-found advantages of new logistical patterns.

The efficiency of ports proves to be a strong indicator of how well each of the ports weathers the short-term losses for days the port is closed, but also the long-term impact of the crisis. Much like economic crises in the past, the Shen attack leads to a reduction in international trading across the globe. Ports in the effected countries suffer negative growth in the years to come with ports in nearby countries suffering from the decrease in trade.[36]

All ports are forced to lower their costs to bolster the reduction of trade and encourage sea shipments. Those ports which can maintain the highest port efficiency with the lowest costs suffer the least. The reduction in cargo growth significantly impacts the value of imports and exports, which also decline. It takes the ports roughly three years to return to the container throughput volumes recorded before the attack.

New regulations are put forward by the World Shipping council which require cyber safety training in ports and on vessels. Hefty fines are put in place by government bodies which fine ports that suffer from cyber-attacks and force shipments to reroute, placing the costs of rerouting on the port as well as the fine itself. New trade partnerships and agreements spring up between affected economies, strengthening ties and altering the geopolitical landscape.

[36] Wang 2014

Sectoral impacts on directly affected countries

The economic impacts on all countries affected by the port closures in this scenario are directly related to the reliance of each country's economy on the transportation sector. As discussed previously in this report, the transportation sector, particularly marine shipping, is responsible for large proportions of the world trade.

The sectors which suffer the largest losses will differ by country, depending on their reliance on the Transportation sector. To give insight into the sectors which will suffer the largest losses, an overview of the economies of each of the directly affected countries for each variant has been provided, as the affects would not be the same in each country due to their market profiles.

S1 variant

In the S1 variant of this scenario report, the countries of Japan, Malaysia, and Singapore are directly affected by the virus. An overview of the sectors which would have the highest losses from disruption to the transportation sector for each of these countries has been provided below.

Japan

24% of the economic input Manufacturing receives comes from the Transportation sector, so this is a close sectoral relationship. It shows that manufacturing is heavily reliant on maritime infrastructure for the internal movement of goods within Japan. This can be understood through the lens of Japan's geography; the Japanese archipelago constitutes 6,852 islands.[37] In combination with the distribution of high population densities along the coast,[38] these factors render other modes of transportation less efficient, creating the sectorial reliance seen.

The Real Estate / Property / Construction sector is the fourth most impacted sector for Japan because of the construction industry's reliance on shipping and rail for the movement of construction goods like timber, scaffolding, prefabricated components, and so on. Japan's construction technology is among the most developed globally, fuelling continuous competitive design, research, and development of construction projects.

Figure 14: Proportions of direct economic losses for the Top 5 affected sectors in Japan (76% of direct economic losses to Japan)

Interestingly, Entertainment & Media, though not in the top 5, is the next most impacted sector in Japan, accounting for 3% of direct economic losses to the region. The Tourism & Hospitality industry is the seventh most impacted sector in Japan, accounting for a similar proportion of the loss.

Global impact from port closures in Japan

The five countries most impacted by port closures in Japan are the USA, China, the Republic of Korea, the Republic of China (ROC) and Hong Kong Special Administrative Region of the People's Republic of China. In 2017, 32% of Japan's exports to the USA were cars and 7.2% of their exports to China were electronic integrated circuits, indicating a significant knock to the Manufacturing sector in these trade partner countries.

[37] "How Many Islands Are There in Japan?" n.d.

[38] Geocoops, n.d.

Malaysia

22% of Malaysian exports to Singapore are electronic integrated circuits and 16% are refined petroleum oils. However, a significant 50% of Malaysian exports to China are electronic integrated circuits. 30% of Malaysia exports to Japan are petroleum gases and 31% of Malaysian exports to the USA are again electronic integrated circuits and, interestingly, 14% are telephones.[39] The reliance on exports from the energy sector makes the mix of affected sectors slightly different from the other five economies discussed. The Energy and IT - Hardware sectors suffer notably more, and Manufacturing is still adversely affected. The Transportation sector still feels the brunt of the Shen attack due to shipping being directly affected, which in turn affects Retail distributors and end consumers for food and household goods.

Sectors that still suffer heavily but are not in the top 5 for Malaysia include all three financial sectors, Banking, Insurance, and Investment Management, each carrying approximately 3% of the direct economic loss for the region.

Figure 15: Proportions of direct economic losses for the top 5 affected sectors in Malaysia (69% of direct economic losses to Malaysia)

The Strait of Malacca to the west of Malaysia is a major chokepoint for global food trade, particularly for grain throughput for western markets. A quarter of global soybean exports transit through the strait to satisfy the demand in China for animal feed. 108 million tonnes of grain are transported by cargo ships through the strait annually.[40] In the event of the Shen attack, this chokepoint that relies heavily on ship movements from Singapore, Malaysia, and China, will be hindered, compromising the global food supply and threatening political instability.
The Strait of Malacca is a critical sea lane for the energy sector - 27% of all seaborne-traded oil passes through the strait each year. A reduction in oil transiting through the strait may also have a destabilising effect on the region.

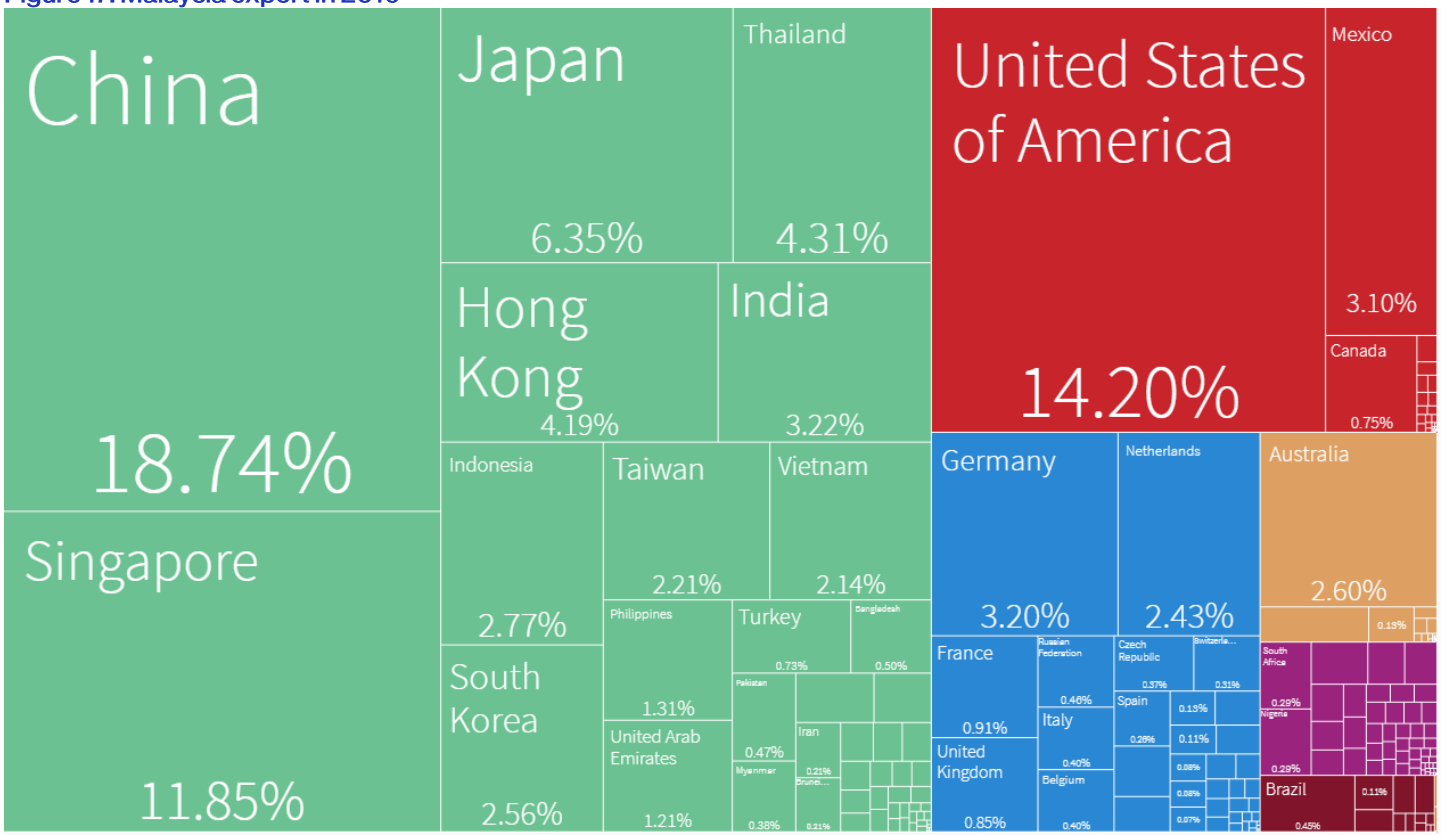
Figure 16: Global maritime chokepoints for food trade[41]

Global impact from port closures in Malaysia

[39] HarvardCID 2016
[40] Bailey and Wellesley 2017
[41] Bailey and Wellesley 2017

Malaysia's top maritime trading partners in 2017 were Singapore, China, the USA, Japan, and Thailand.[42] These trading partners will be adversely affected by any restriction to day-to-day shipping functions out of Malaysia.

Figure 17: Malaysia export in 2016[43]



Singapore

Transportation and Manufacturing are the two hardest hit sectors for all countries in all scenario variants. For Singapore, Malaysia, and The Republic of Korea (included in S2), Transportation is the hardest hit sector. Because of its heavy reliance on seaborne trade and maritime connections due to its geography, the Transportation sector is a key lifeline to multiple other sectors, including Retail, Manufacturing, and Pharmaceutical distributions. For Singapore, the Transportation sector suffers 45% of all direct economic losses, greater than any other sector in any other country in this study.

Figure 18: Proportions of direct economic losses for the top 5 affected sectors in Singapore (79% of direct economic losses to Singapore)

Other sectors that suffer greatly are Business & Professional Services, accounting for 5% of direct economic losses, and the Real Estate / Property / Construction sector, accounting for 3% of direct economic loss.

[42] UNCTAD 2017
[43] The Observatory of Economic Complexity 2017

Global impact from port closures in Singapore

The five territories most impacted by port closures in Singapore are China, Hong Kong Special Administrative Region of the People's Republic of China, Malaysia, the USA, and Indonesia. This is at a tier 2 level, the first rung of the downward supply chain. Singapore exported $51.7 million to China by sea in 2017.[44] In 2017, Singapore's primary exports to China were predominantly electronic integrated circuits (40%) and refined petroleum oils (7.5%),[45] so Manufacturing and IT- Hardware will suffer severely in this scenario.

S2 variant

The countries affected in the S2 variant of this scenario report include all the previously listed countries as well as ports in The Republic of Korea. An overview of the sectors which would have the highest losses from disruption to the transportation sector for The Republic of Korea have been provided below.

The Republic of Korea

Other than the inevitable impacts to the Transportation industry due to the port closures, Transportation, Manufacturing, Retail, Business & Professional Services, and Pharmaceuticals suffer the greatest losses in The Republic of Korea. The largest share of exports from The Republic of Korea for any single item are electronic integrated circuits (11%) followed by Information and Communications Technology (ICT) at 7.78% in 2016, demonstrating the size of the country's Business & Professional Services sector.

A large portion of exports are also from transport, cars, cargo ships and similar vessels, and parts of motor vehicles, pushing impacts to the Transportation sector to the number one spot of directly affected sectors. The Republic of Korea also exports a range of machinery for use in the medical industry, such as liquid crystal devices, ventilation equipment, optical fibres, equipment for temperature change and materials, measuring instruments, centrifuges, refrigerators, medical instruments and so on, hence the impact to the Pharmaceutical sector.

Other hard-hit sectors in The Republic of Korea include the Defence & Military Contractor sector, which carries 3% of the direct economic cost for the region and IT - Hardware, accounting for 3% of the direct economic loss.

Figure 19: Proportions of direct economic losses for the top 5 affected sectors in The Republic of Korea (77% of direct economic losses to The Republic of Korea)

Global impact from port closures in the Republic of Korea

While it has a comparatively smaller GDP to the other directly impacted countries, port closures in The Republic of Korea have a significant impact to their top five exporting markets of China, USA, Vietnam, Hong Kong Special Administrative Region of the People's Republic of China, and Japan. 31% of their exports to China in 2017 were electronic integrated circuits, so any constraints placed on the shipment of these goods would have negative implications for the Manufacturing sector.

[44] UNCTAD 2017
[45] HarvardCID 2016

X1 variant

The countries affected in the X1 variant of this scenario report include all previously listed countries as well as China. An overview of the sectors which would have the highest losses from disruption to the transportation sector for China has been provided below.

China

As China is the world's largest manufacturing economy and exporter of goods,[46] it is not surprising that the main industries affected in China from the port closures due to the Shen attack are Manufacturing, Transportation, Retail and Real Estate / Property / Construction.

China has a notably diverse range of export product sectors and items not seen with the other four countries in the X1 scenario variant. The products accounting for the greatest share of exports are shown in **Error! Reference source not found.**Table 7.

Table 7: Top 5 products exported from China in 2017[47]

Product	% share of exports
Broadcasting Equipment	9.6%
Computers	6.1%
Office Machine Parts	3.8%
Integrated Circuits	3.3%
Telephones	2.6%

Most exports come from the Manufacturing industry, displacing Transportation as the most impacted sector.

Sectors that suffer significant losses in China, though which are not amongst the top 5 most impacted sectors, include Food & Agriculture, accounting for just under 3% of the direct economic loss for the region, and the IT - Hardware sector, which accounts for just over 3% of the direct economic loss.

Figure 20: Proportions of direct economic losses for the top 5 affected sectors in China (74% of direct economic losses to China)

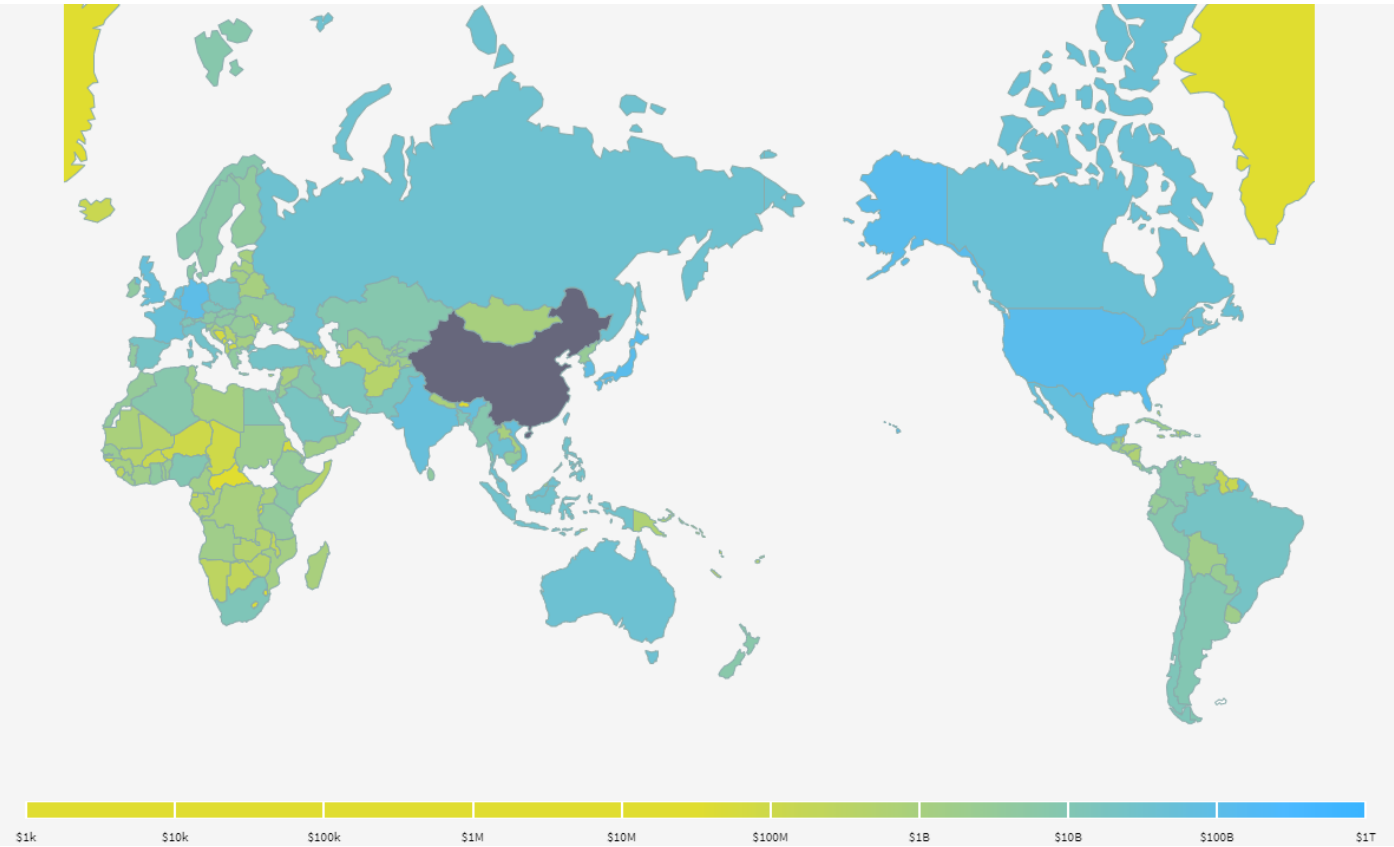
Global impact

The international reach of port closures in China is felt throughout the word with the countries of USA, Hong Kong Special Administrative Region of the People's Republic of China, Japan, The Republic of Korea, and Vietnam suffering highest direct losses from the closures.

[46] Sims 2013

[47] The Observatory of Economic Complexity 2017

Figure 21: Where did China export to in 2016?[48]



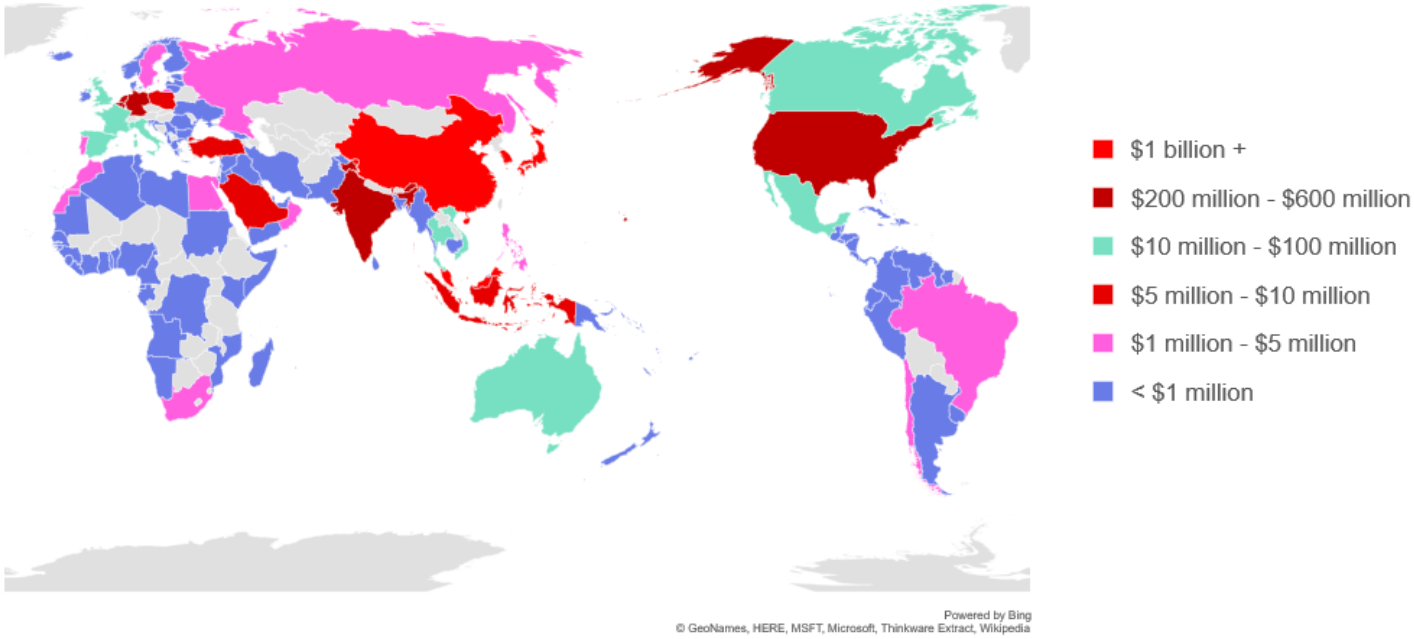
[48] HarvardCID 2016

Global and regional economic losses

5. Global and regional economic losses

Although the Shen virus only directly affects ports in the Asia Pacific region, economic losses are felt around the world from this scenario due to the global nature of the maritime supply chain.

Figure 22: Map of total global economic losses from Shen for X1 (direct and indirect)



Categories of loss

Several categories of financial loss can be expected to result from a cyber-attack of this nature. The size and duration of the attack, including the extensive theft that occurs in the months preceding the triggering of the Shen virus, lead to losses in several areas. Some of these losses are modelled in this report where research indicates substantial costs. The report makes clear which losses have been modelled and which losses are addressed qualitatively.

Figure 23: Modelled losses

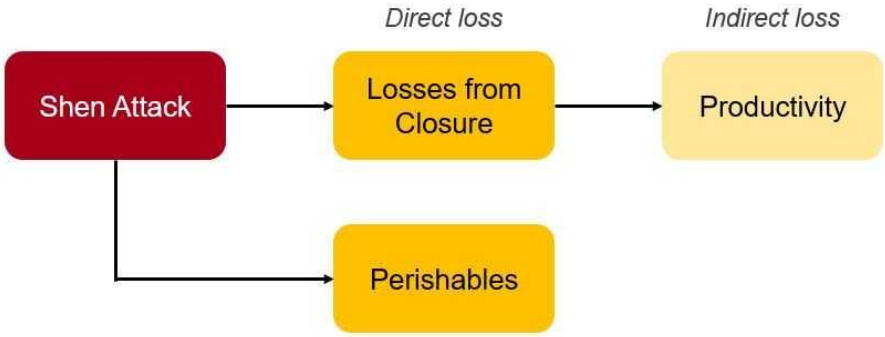
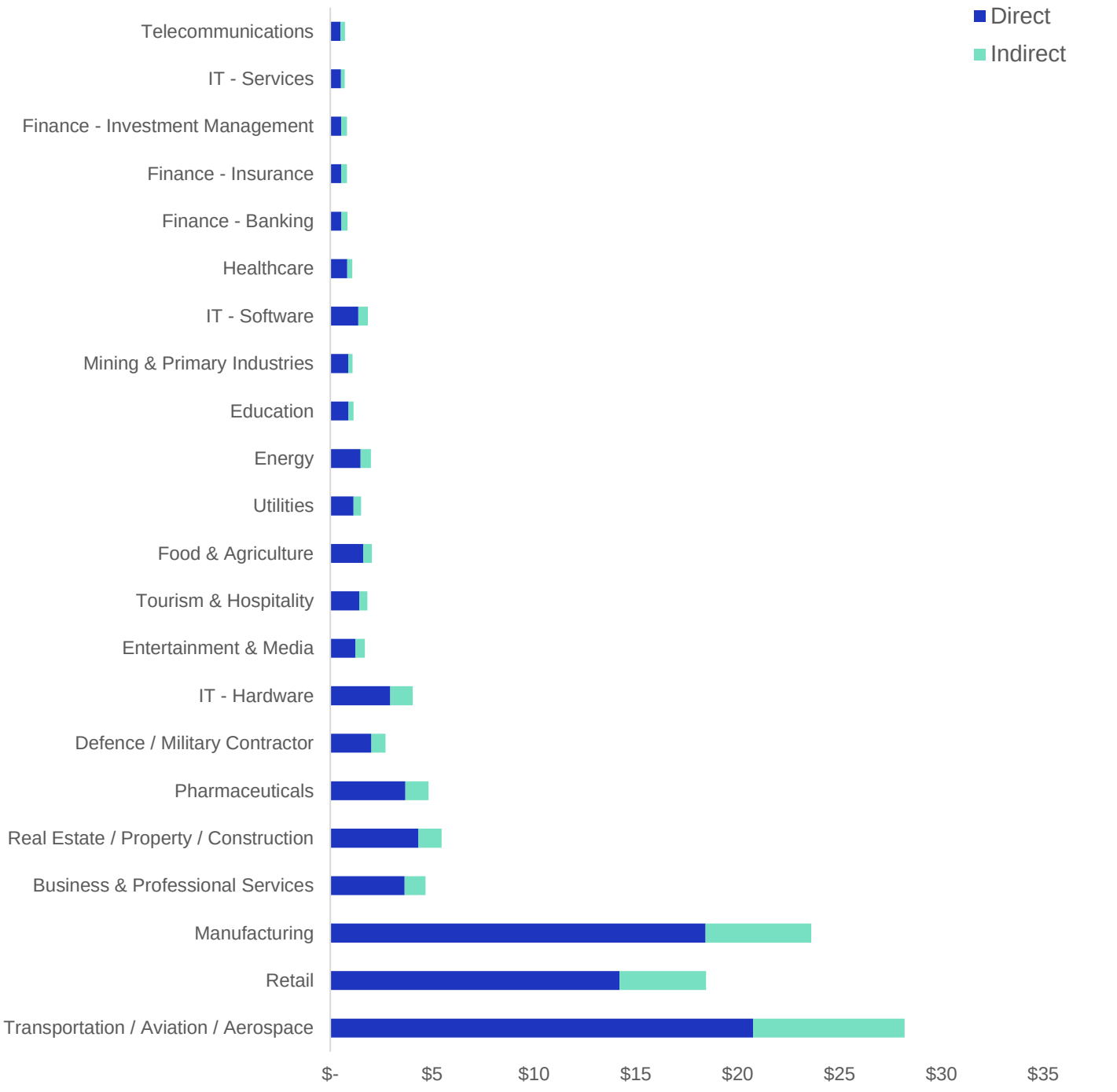


Figure 24: Total global direct and indirect economic losses by sector (X1 variant)



Box 5: 2002 West coast port lockout

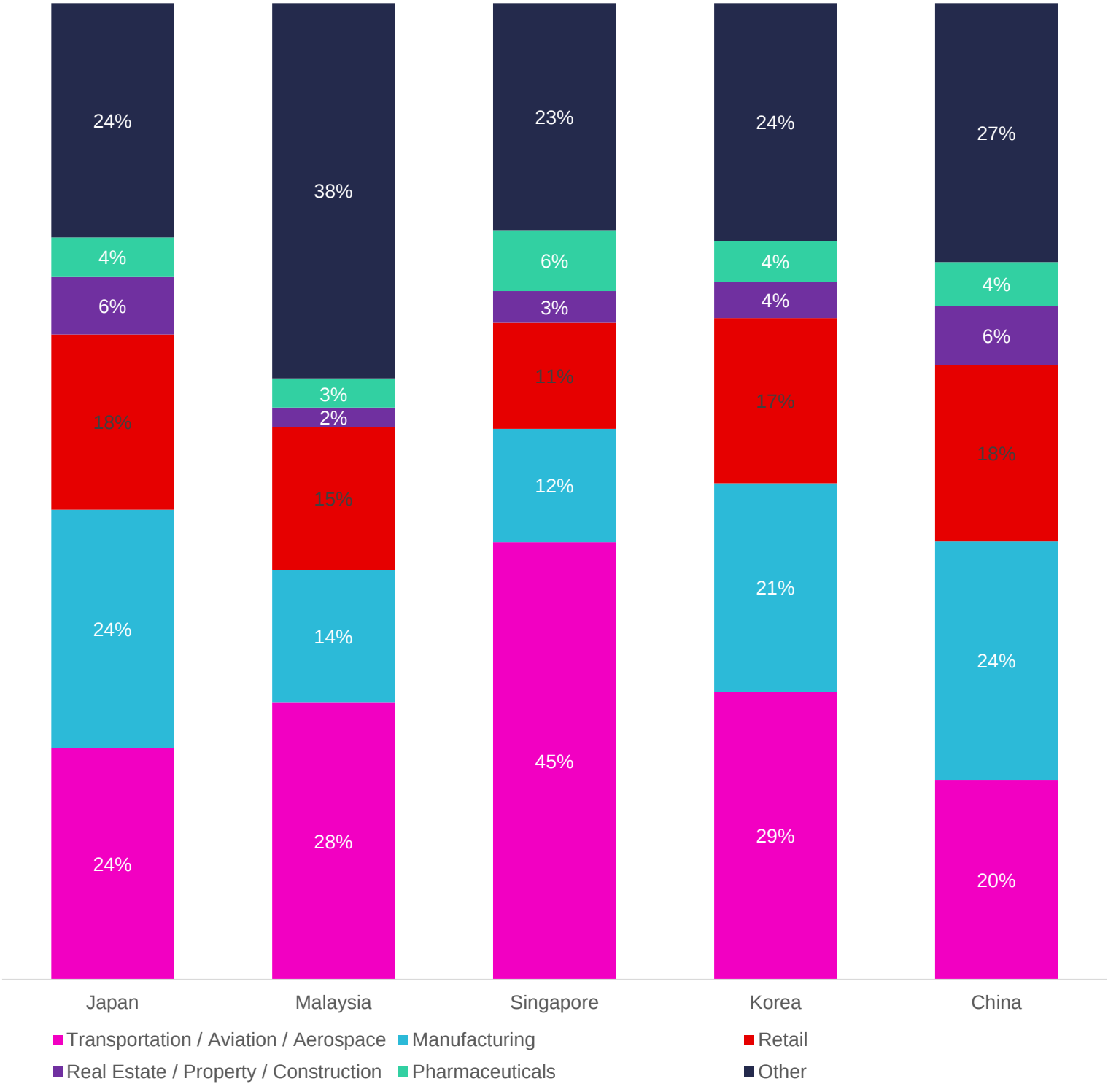
Approximately every five years, the collective bargaining agreements governing the longshoreman labour used at various ports along the West Coast of the USA, expire and the parties are required to renegotiate the contracts. In 2002 the labour contract between the International Longshoremen and Warehouse Union (ILWU) and the Pacific Maritime Authority (PMA) came up for negotiation.

The negotiations stalled into a work slowdown, which prompted the PMA to impose a lockout of dock workers. The impact of this action resulted in an 11-day shutdown of the ports along the West Coast, with estimated costs to the economy reaching $2 billion a day. The total cost of this shutdown, adjusted for inflation for 2019, is estimated as $31 billion.

Direct losses

Losses occurring as a direct result of the Shen virus and the cybercrime group's activities fall under the umbrella category of direct losses. This includes business interruption, stolen goods, and spoiled goods.[49] These three subcategories of direct loss have been modelled. Figure 25 shows the sectors with the largest direct losses in each of the countries with infected ports.

Figure 25: Top 5 sectors most heavily dependent on the transportation sector in each directly affected country



[49] Box: *Hall 2004*

Port closure

The Shen attack forces port closures because of operational dependencies on the infected software. Shutdowns lead to financial losses from productivity slowdowns and business interruption, also referred to as productivity loss or losses from closure or port shutdown. These are any disruption of on-site port activities and operations, such as personnel not being able to complete day-to-day tasks, vessels not being able to move in and out of port on a pre-set schedule, and containers being delayed in routine movements between barges, ships, trucks, and storage facilities.

The outage length varies for each country based on a range of indicators including port closure precedents. The variation of outage length for the ports in this scenario was calculated using an outage metric which incorporates the size of the port, the technical efficiency, as well as the annual TEU.

Perishables

A proportion of goods shipped in refrigerated containers, also known as reefers, are required to have temperature control and traceability as products have a limited shelf life. This temperature range varies according to what the product is and is maintained as part of the cold chain, which is the overall temperature management during the products supply chain cycle. The Shen attack that scrambles the container management systems also scrambles the temperature data logs, creating a gap in the traceability of the cold chain. This gap in the data means that the cold chain fails to meet the quality assurance criteria as the temperature cannot be verified over the period from the release of the virus to full recovery of the port. At some container terminals, workers can use Remote Container Management (RCM) devices that have digital displays to verify the temperature logs. However, the data sent from these devices is compromised because of the centralised database and port management system. Further, uncertainty around the extent of the targeted attack casts doubt on the accuracy of available data, particularly historical data from the transit itself. As a result, products contained within the containers are compromised and need to be disposed of.

Note on pharmaceuticals

The 2018 market for pharmaceutical cold chain logistics was $15 billion, with over 12% year-on-year growth forecast.[50] The global pharmaceutical logistics market, which includes temperature sensitive pharmaceuticals, is valued at $64 billion.[51] The fastest mode of transport for time-sensitive pharmaceuticals is still air travel. However, only half a million metric tons of pharmaceuticals are shipped by air annually, compared to 3.5 million tons by sea. This is because shipping by sea is 80% cheaper and sea freight has fewer product handoffs, making it the more affordable and more reliable option. There are other benefits surrounding the shift to seaborne rather than airborne pharmaceuticals: customs administration can be done while in transit; the carbon footprint of ocean transport is 4% the size of air travel's; and if there is a delay, then pharmaceutical cargo becomes part of a "floating warehouse" and is recognised as inventory.[52]

In the Shen scenario described in this report, time-sensitive, temperature-controlled pharmaceuticals are broadly included in the Perishables category. Overall, perishables make up a small proportion of the total economic loss, between 0.07% and 0.75% for the directly affected countries, so the pharmaceutical segment has not been modelled separately.

Indirect losses

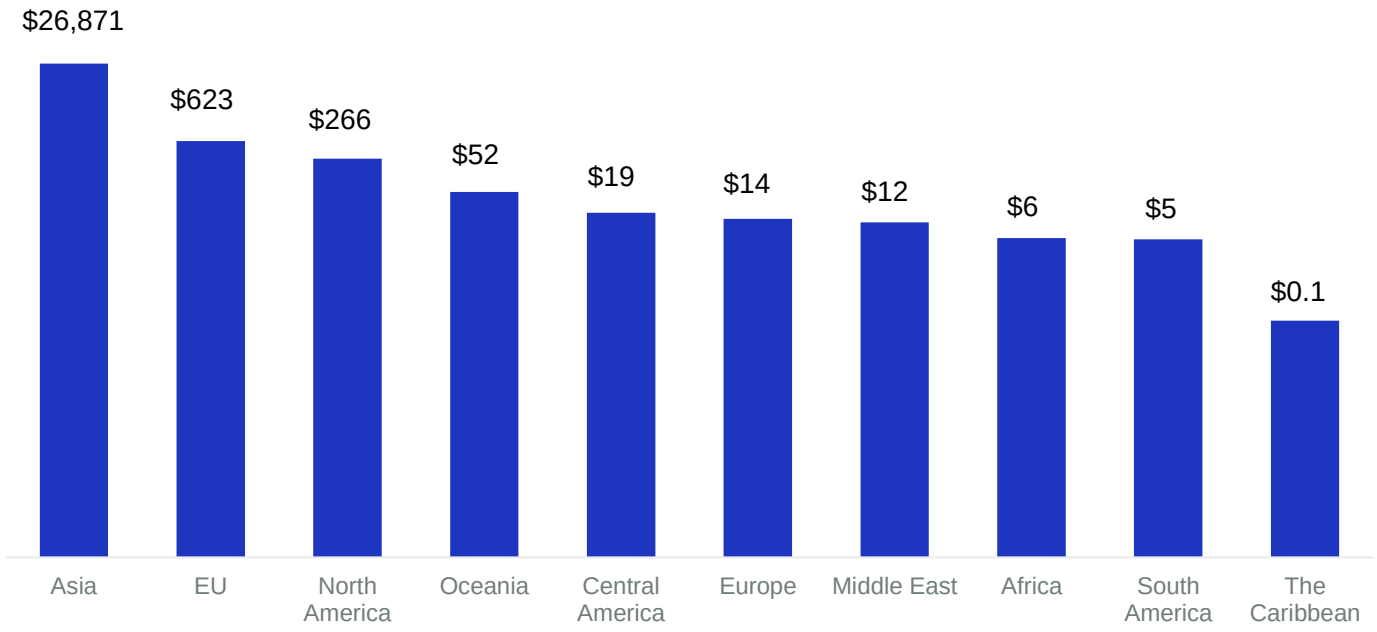
The integration of national economies into a global economic system has resulted in substantial levels of growth in trade between countries. In today's global economic system, countries exchange final products and intermediate inputs creating an intricate network of global economic interactions.

The Shen virus results in an interruption in global economic trade creating substantial economic losses. These losses are incurred by various companies as their business continuity is affected. The manifestation of this loss is dependent on the sector and goods transported.

The indirect losses modelled in this scenario are modelling the productivity losses for each country that has bilateral trade with the affected ports in their respective countries. A daily loss is calculated for each affected country based on the GDP, merchandise trade, world container share percentage, country exports,[53] and bilateral trade index of the 155 countries for which data is available.[54]

[50] Pharmaceutical Commerce 2018
[51] Controlant 2018
[52] Basta 2018
[53] World Integrated Trade Solution 2017
[54] UNCTADstat 2018a

Figure 26: Total indirect losses by region ($million)



In this figure a logarithmic scale is applied to account for the large differences across territories.

The indirect losses presented in this report are cautious estimates. Though they have been modelled extensively, they are not modelled through all levels of the supply chain. For example, the direct impact to ports in China is expected to impact the US economy. This has been modelled and these losses are included in the report. However, the tertiary impact that the impact to the US economy has is not modelled. As a result, the indirect losses shown here can foreseeably be significantly higher as the impacts compound through multiple supply chain tiers.

Productivity

The production of goods and services, their supply, distribution, and post-sales activities is coordinated by people and activities across geographies in what is known as the global value chain. Each step in this sequence of a product's manufacturing to its commercialisation presents a productive, or value added, activity, and often each step is managed by a different company in a different location. Because of task-specialisation and integration into a highly coordinated, global business model, these connections generate far more value together than the value offered by their constituent parts and processes. This is especially true for manufacturing, distribution, and retail sales.

Two primary categories of goods emerge from the global value chain: final goods and intermediate inputs. Final goods are produced by combining local intermediate inputs, whereas intermediate inputs are produced by combining differentiated inputs and labour so that the economy features roundabout production. Final goods are sold locally to consumers in a typically competitive market, although this is not always the case where tariffs on international goods and market regulations can impede the competitiveness, whereas intermediate inputs are produced and distributed worldwide by monopolistically competitive firms. Since only intermediate inputs are traded, firms combine capital and labour with intermediate inputs supplied by upstream firms.

Following the Shen virus, the productivity of firms whose supply chains are affected declines. Individual firms produce at lower rates, which further reduces trade. This affects the firm directly and this productivity effect is amplified along all production chains as the suppliers of suppliers are similarly affected.

Bilateral trade

The net sum of exports and imports between countries enhances or restricts trade. Several metrics exist for determining the intensity of trade between countries, with one of the most useful being a bilateral trade index. A bilateral trade relationship exists between most pairs of countries that engage in trade globally. This metric is typically defined on a country level and defines the exported goods to another country that also import goods from the same country. A higher bilateral trade index indicates that the two countries benefit from each other in their trade relationship and enjoy a more integrated economic system.

The usefulness in cross-country comparisons of trade is typically limited since the measure does not account for the effect of economy size on trade level, as different sized economies can be expected to trade in proportion to the size of their economies.

Trade intensity is strongly linked to geographical distance and can be one of the most imposing restrictions to trade. This limitation exists as defining the geographical relationship can be challenging when viewing this through the lens of transport as they are facilitators of trade and not the actual trading partners. Bilateral trade is therefore a useful proxy in this model for geographical instance, particularly when considering the fact that this cross-country comparison does not account for economic size. The economic size is represented by various maritime statistics that allow a gravity model to be employed to calculate the productivity shock due to the delay in trade for supply chains.

Factors not modelled

Mitigation strategies & recovery rates

In determining port recovery rates, a port Efficiency Score was used for each individual port in the Shen attack. This considers the rate at which a port could be expected to recover based on existing port productivity, cargo handling at berth, infrastructure characteristics, terminal area, and optimum container throughput, amongst other measures.

Many other variables influence the recovery rate, such as operational decisions in where port workers are deployed, the capacity of the workforce, types of activities that can be done manually when automatic or online systems fail, and other dependencies such as the number of partner companies that rely on the container terminals operating at full capacity. Not all these variables could be controlled for in the Shen modelling because not all variables can be known for all ports. However, there are many mitigation strategies ports can employ in the event of a cyber-attack, which may result in them resuming activity at faster rates.

Port authorities can prepare for and react to emergency situations in a range of ways. Some mitigation strategies may involve adjusting production schedules, performing preventative maintenance, or slowing the rate of production in order to avoid a total shutdown of facilities.

They could employ alternative transportation routes or modes in conjunction with arranging goods from different suppliers. Economic activity would be redistributed as these emergency measures take effect and consumers adjust their purchasing behaviour.

Some ports will have better developed emergency response plans than others, and some will defer to national plans rather than focus on locally development ones, which will impact the nature of the response. Appropriate education of port personnel and the existence of regulations to monitor and mandate these plans can be expected to affect the speed of recovery and the resulting cost.

A full assessment of these mitigation strategies and the macroeconomic variables they would influence is beyond the scope of this report and so has not been modelled.

Additionally, some sectors may gain work when required to provide services to the impacted ports. Business and Professional Services, for example, will suffer losses due to the attack but will also be in high demand following it. The current model used in the report only captures value destruction, not generation.

Blockchain

Technically forming part of a company's mitigation strategy, Blockchain technology can be incorporated into existing workflows for high levels of data security and protection.[55] Port Authorities are gradually moving into the Blockchain space. For example, Jade Logistics has partnered with Augen Software Group, headquartered in New Zealand, to develop supply chain applications using new Cargo Chain technology throughout Southeast Asia.[56] This will lead to improvements in data sharing, improved data encryption, and address issues of scalability.[57]

Blockchain technology is gradually being trialled, adopted, and rolled out across various ports in the region, but the market is still niche and fragmented, with little information available on which port authorities have partnered with which software providers. For this reason, the benefits of Blockchain technology are not included in Shen scenario modelling.

Supply chain

Productivity disruption or inability to export has been modelled in this report in lieu of supply chain losses in the economic losses section. The complexity of global supply chain prevents one from accurately creating an upper bound of loss and thus an accurate loss number. The impact to countries with close trading relationships to the directly affected countries is modelled as productivity loss from delayed goods, represented by the contingent business interruption (CBI) losses detailed in the insurance section.

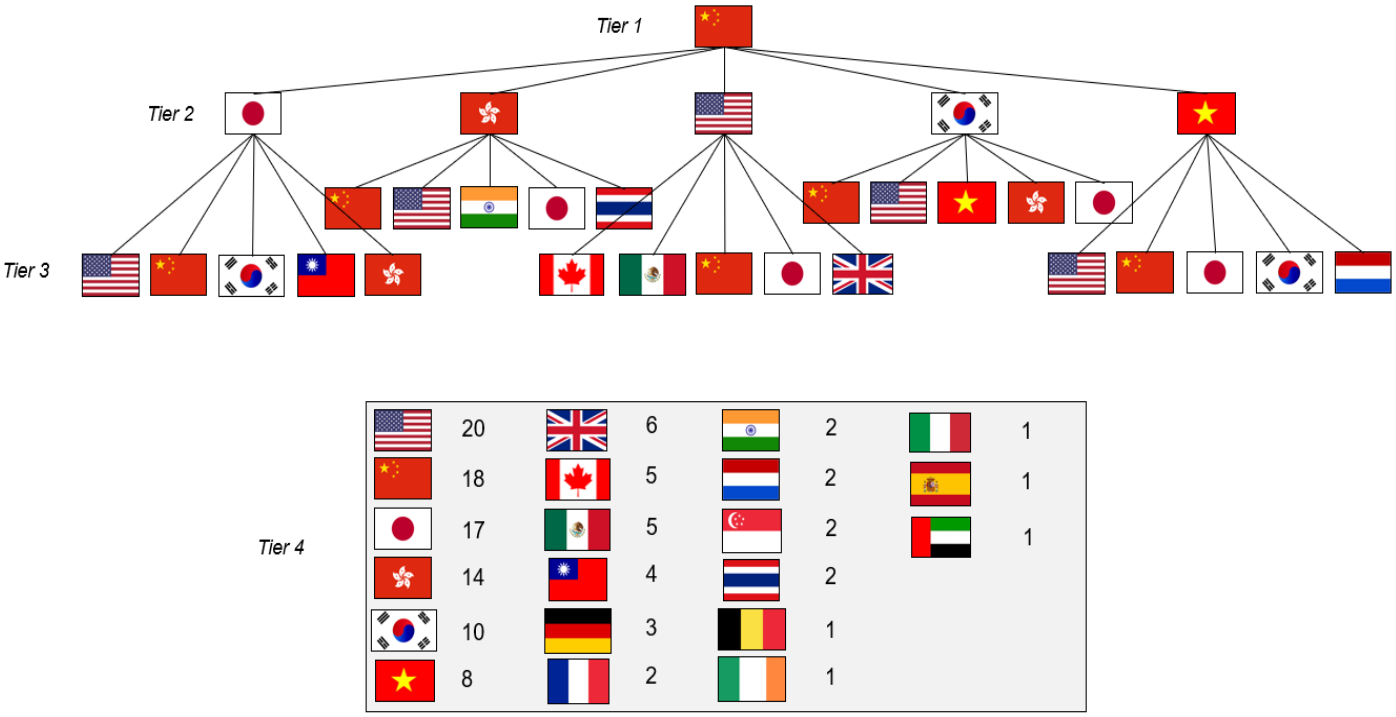
International trade comprises complex production chains that cross-national boundaries many times. A disruption to the international flow of goods would adversely affect these production chains. Since the process of acquiring upstream suppliers and downstream customers is a timely and costly process, rebuilding the affected segments after an economic shock would take Supply chain interactions expand outwards and have been assessed down four levels, or tiers. The first tier of impacts are the ports of countries directly infected with the Shen virus with the following tiers suffering supply chain losses.

[55] Baxter 2018

[56] CargoChain 2019

[57] WCN Editorial 2018

Figure 27: Top 5 trading partners for China and their top 5 trading partners



Some strong trading countries, such as the USA and the Hong Kong Special Administrative Region of the People's Republic of China, appear several times.

Insurance loss estimations

6. Insurance loss estimations

The CCRS Insurance industry loss modelling for the Shen Scenario considers the insurance industry exposure arising from both affirmative cyber cover and non-affirmative cyber cover. The loss estimates from this model reflect likely pay-outs for the global insurance market in 2019. This structure, and the associative estimations, result from research into recent publications around insurance penetration, policy structures, and extrapolation from historical precedents.

General model assumptions

The losses modelled are categorised first by the principal parties of those who have incurred losses. The seven parties are; the port operators, the cargo content owners, the ship owners, the companies who designed and manage the infected port management systems, the companies involved in the cargo handling and logistics who are infected, the company responsible for the ship management system, and the companies who are indirectly affected.

CCRS calculated the losses based upon port specific statistics forming an insurance profile for each port, primarily using the daily TEU throughput, days shutdown, and the losses incurred by the port due to this shutdown. The port specific insurance profile is then tabulated through several lines of insurance found in Table 8.

A distinction for the insurance claims is whether the policy claimed on relates to a cyber affirmative or a silent cyber policy. The report uses the following standardised definitions which are used by CCRS when discussing these two types of policies.[58]

- Affirmative Standalone Cyber Cover – Specific standalone policies for data breach, liabilities, property damage, and other losses resulting from information technology failures, either accidental or malicious.
- Affirmative Cyber Endorsements – Cyber endorsements that extend the coverage of a traditional insurance product, such as Commercial General Liability.
- Non-affirmative Cyber Exposure: Gaps in Explicit Cyber Exclusions – Non-affirmative Cyber Exposure: Gaps in Explicit Cyber Exclusions – There are a range of traditional policies, such as commercial property insurance, that have exclusion clauses for all losses resulting from "loss, damage, destruction, distortion, erasure, corruption or alteration of Electronic Data [as defined]". The clause then provides a write-back of coverage for the perils of fire and explosion resulting from loss (etc.) of Electronic Data.
- Non-affirmative Cyber Exposure: Policies without Cyber Exclusions – Many insurance lines of business incorporate 'All Risks' policies without explicit exclusions or endorsements for losses that might occur via cyber-attacks.

The global insured losses resulting from the Shen virus are shown Table 8. This table outlines the insured industry losses by type of claimant, coverage, and the scenario variant. It is assumed that some of the losses will be a consequence of subrogation. Within this scenario, criminals are not engaging in terrorism or warfare. War exclusions are not applied.

[58] CCRS 2018

Table 8: Insurance industry loss overview group by claimants, $millions

$ Millions			S1	S2	X1
Class of insurance	**Type of insurance**	**Cyber policy type**			
Port Operators					
Cyber	Business Interruption	Cyber Affirmative	$594	$813	$1,407
Commercial Property	Business Interruption	All Risks	$497	$646	$1,240
Liability	Directors and Officers	All Risks	$85	$116	$235
Cyber	Incident Response costs	Cyber Affirmative	$188	$266	$553
Cyber	Regulatory and Defence Coverage	Cyber Affirmative	$146	$202	$464
Cyber	Reputational Risk	Cyber Affirmative	$62	$96	$227
Cyber	Data and Software Loss	Cyber Affirmative	$17	$23	$41
Cargo Content Owners					
Marine	Cargo	Cyber Affirmative	$82	$104	$237
Ship Owners					
Marine	Freight, Demurrage and Defence	All Risks	$30	$45	$74
Port Management System Software					
Liability	Directors and Officers	All Risks	$119	$178	$296
Liability	Technology Errors and Omissions	All Risks	$71	$107	$178
Logistics and Cargo Handling Companies					
Liability	Directors and Officers	All Risks	$161	$241	$402
Cyber	Business Interruption	Cyber Affirmative	$48	$72	$120
Commercial Property	Business Interruption	All Risks	$192	$288	$480
Cyber	Data and Software Loss	Cyber Affirmative	$142	$212	$354
Ship Management Company					
Liability	Technology Errors and Omissions	All Risks	$198	$198	$198
Liability	Directors and Officers	All Risks	$10	$10	$10
Cyber	Data and Software Loss	Cyber Affirmative	$30	$30	$30
Supply Chain Companies					
Commercial Property	Contingent Business Interruption	All Risks	$868	$1,194	$1,563
Cyber	Contingent Business Interruption	Cyber Affirmative	$104	$144	$187
Total Insured Losses			$3,641	$4,983	$8,294

Values have been rounded to the nearest whole number, so total figures may not add up.

Cyber exclusions

This scenario recognises that cyber exclusions are likely to be applied to marine policies. A notable exclusion which is anticipated to be applied is the Institute Cyber Attack Exclusion Clause (CL380). CL380 excludes insurance cover for risks occurring because of cyber-attacks. The clause reads:

> *"...in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system."*

The clause has been a growing point of criticism within the Marine insurance industry, as it is felt that the exclusion is too broad and does not account for the extent cyber products are currently being used in the marine industry.

There has been a development of new clauses and cyber affirmative products:

- For example, the Lloyd's Market Association (LMA) and Joint Committees have recently released clauses for rig (JR2019-001) and for cargo (JC2019-004) which provide additional clarity to account for the growing integration of cyber technologies. The International Underwriting Associated has also released two new model clauses IUA 09-081 (Cyber Loss Absolute Exclusion Clause) and IUA 09-082 (IUA 09-082).[59]
- Insurers have launched several new affirmative cyber insurance products within the marine industry in response to a growing market need and to comply with a forthcoming update to the International Maritime Organization's marine cyber risk management guidelines [60] Insurers are expected to demonstrate compliance with the guidelines by 2021. The new insurance products hitting the market cover loss of vessel hire and physical damage. These products are offered as part of a package or as a standalone policy.

Within this scenario, marine policies are assumed to have a 50% exclusion rate to account for CL380 and other cyber exclusions. This rate considers the current soft market considerations, and the number of larger brokers who do not support the exclusion. The rate is scaled to account that cyber exclusions may not be standing in cases of consequential losses or may not be broad enough for the proposed cyber event.

From January 2020 Lloyd's have mandated all policies to provide clarity on whether cyber coverage is provided or not.[61] Lloyd's view is that it is in the best interests of customers, brokers and syndicates for all policies to be clear on whether coverage is provided for losses caused by a cyber event. This clarity should be provided by either excluding coverage or by providing affirmative coverage in the (re)insurance policy. We anticipate this will reduce ambiguity in cyber coverages.

Claimant types

Port operators

Port Operators are defined as companies or boards who regulate and manage port and marine services, facilities and activities within their associated jurisdictional waters. Activities includes vessel traffic and navigational safety and security, through regulation on operational efficiency and on the environment. Those ports that are affected by this scenario will have insurance claims arising from the Port Operators to recover a portion of the incurred economic losses.

Cargo content owners

The cargo content owners are either individuals or organisations that have paid for the cargo under a legal contract. From a trade and logistics perspective, cargo is a good that has been traded, bought, or sold, and can include items such as toys, electronics, food stuff, or raw materials. The cargo is often transported in TEU containers and will typically change multiple hands before reaching the owner, as various transportation modes are employed to transport them. Within this scenario, the system disruption causes extensive delivery delays, and causes perishables to spoil. Within the scenario, the cargo content claimants are solely perishable cargo owners. Perishables are assumed to account for roughly 7% of total cargo turnover.

Ship owners

Ship owners are the people or organisations responsible for the ownership and operation of the vessel. In a commercial setting, ship owners may move cargo and charge a freight rate. Ship owners regularly hire crew and captain to run the

[59] Banner 2019

[60] *Insurance Journal 2019*, International Maritime Organization (IMO) 2017, Malynn 2019

[61] Market Bulletin Y5258

ship and maintain daily operations. Within this scenario, the ships docked at affected ports will have substantial delays in loading and unloading cargo, and charterers will have possession of the vessel for longer than expected. This will result in accumulated demurrage charges, in which ship owners will require legal representation and expert advice.

Port management system

The Port Management System is a software application that supports the administration and operations of port operators in a range of tasks. The primary activity of this software is managing and recording all activities occurring in a port, thus supporting the business processes of the port authority. The system is used to demonstrate compliance to national and international regulators, support the port's financial obligations, and host communication between service providers, terminals, waste collectors, ship chandlers and government. The software provider of the port management system will be held liable for the software's vulnerability, manipulation, and transmission of the virus.

Logistics and cargo handling companies

Logistics and Cargo Handling Companies are responsible for the planning, execution and control of the movement of cargo and goods, information, and services. Logistics and Cargo Handling Companies connect the marine cargo industry with wider supply chains. Within the scenario, the Port Management System transfers the virus to Logistics and Cargo Handling Companies through shared data, compromising some record systems and impacting their operations.

Ship management company

A Ship Management Company is a company independent of the owner of the ship which maintains and operates the vessel. The main function of a ship management company is to provide ship owners with support including supplying and managing crew, technical and software support, live monitoring systems, and other services such as inspections and ship maintenance. In this scenario, the ship management company's software is compromised and introduces the virus to the port management systems. They are the key target of liability claims in this scenario.

Third-Party organizations indirectly impacted

Third-party organizations who are indirectly impacted considers those who are impacted further along the supply chain. Both upstream and downstream supply chain shocks occur due to a disruption or failure of cargo services. Companies whose business is reliant on the cargo entering or leaving the port face an interruption of products and services.

Loss coverage categories

Business interruption

Business interruption claims occur when profits are lost, or extra expenses are incurred due to asset damage. Traditionally, for business interruption insurance to be triggered a requirement is placed upon the policyholder for physical damage to have incurred. As business interruption is evolving to include cyber events, data can be classified as property in some policies, meaning that digital asset losses can trigger a claim. In addition to the claims being made on affirmative cyber policies, there might also be exposure in the traditional property books under business interruption, as has been seen in the recent NotPetya attack.[62]

Notably, not all jurisdictions or insurers recognise data as property which can trigger a business interruption claim. The interpretation of data property varies widely across the insurance industry. In the current environment there is movement to address non-affirmative wordings to clarify intent of coverage.

Within the scenario, the virus corrupts the ship management system, and then later the port management system and Logistics and Cargo Handling Companies' systems, scrambling the information stored about the cargo. Port operators and Logistics and Cargo Handling Companies are forced to temporarily halt their operations, resulting in a reduction in productivity and loss of revenue.

Vessels awaiting to unload their cargo at the affected ports may be diverted to other ports, depending on the cargo type and destination. As these companies are not able to maintain their regular commercial operations, they face financial losses attributed to business interruption.[63][64][65]

Box 6: Ambiguity in cyber business interruption coverage

The WannaCry and NotPetya cyber events in 2017 highlighted the growing need for cyber business interruption coverage, as large major corporations like Maersk, FedEx, Deutsche Bahn, and Renault saw several-day disruptions of critical internal IT systems. Not all cyber BI policies are alike in the type of events they cover. Some policies cover all three of the following event triggers while others cover only one.

1. *Malicious Threat Actor* – business interruption cover where the threat actor has malicious motivations, such as the intent to cause harm or property damage to the target. Malicious motivations are typically associated with cyber criminals or nation-state threat actors. To receive a claim award, it is key that insureds have wording for malicious threat actors.

2. *System Failure* – in this case first party business interruption cover could result from an accident by an employee that causes an unplanned disruption. It is also offered as a third-party coverage for when an external event causes an unplanned outage. In both cases wording suggests that the cause of the outage must be negligence.

3. *Service Provider* – business interruption cover resulting from an unplanned event at an external IT service provider, other non-IT provider and/or utilities. This BI coverage potentially overlaps with CBI coverage. As not all insurers have adapted this IT supply chain disruption into their BI coverages, CCRS choose to model this loss separately as CBI.

Further, it is important to review any exclusions on cyber BI policies that may limit cover. "Many insurers have "failure to patch" exclusions, which exclude any and all coverage for any and all damages in the event that the vulnerability had been previously identified and not patched."

[62] Box 6 'Ambiguity in cyber business interruption coverage
"Petya Cyber Industry Loss Passes $3bn Driven by Merck & Silent Cyber: PCS - Reinsurance News" 2018

[63] Text is taken directly from the 2019 Bashe attack: Global infection by contagious malware Report (Cambridge Centre for Risk Studies, Lloyd's of London, and Nanyang Technological University 2019)

[64] Buck 2018; JLT 2018a

[65] Aon Risk Solutions, n.d.

Directors & Officers

Directors and Officers (D&O)[66] liability insurance covers the costs of compensation claims made against directors or key managers of a business for alleged wrongful acts. Examples of wrongful acts can include breach of trust, breach of duty, error, or failing to act in the best interests of the company, its employees, and its shareholders.

A scenario as severe as one caused by the Shen virus has the potential to cause shareholders to seek payment for corporate losses due to lack of readiness plans, and potentially the poor execution of readiness plans resulting in a share price impact. Once investigation of the chain of liability is resolved for the individual port operators, the liability insurance would cover a proportion of the legal costs and judgements awarded. D&O claims are also assumed for port operators, port management systems, Logistics and Cargo Handling Companies, and ship management systems executives. This stems from the assumption that key managers do not properly report the system's vulnerabilities or respond to the virus in a timely and effective response.

Box 7: D&O insurance

Directors & Officers (D&O) insurance is most commonly seen in U.S. markets, and has historically been less pronounced in Asia. In recent years there has been a growing demand of D&O insurance within Asia, and increasingly regulatory actions are being taken. Asian D&O Insurance is projected to grow further in the future, especially as regulatory enforcement becomes more aggressive.

This scenario intends to stress the potential impacts of the rise of D&O claims and speculates an aggressive 50% insurance penetration for Port Operators. The scenario assumes that Port Management System Software, Logistics and Cargo Handling Companies, and Ship Management Companies are all headquartered in the United States where D&O insurance is more common.

Incident response

Incident response refers to the cost of responding and managing the impact of a cyber event. Example costs include the hiring of consultants, or privacy notification expenses. Within the scenario, port operators must quickly respond to the virus, and investigate the extent of system damage. The initial technical response will be contained to reverse engineering the virus to potentially reverse the scrambling of the shipping manifests. After subsequent attempts the response will shift to one of managing the process of physically sorting the containers and manually checking the shipping manifests. Extra resources are required for this process and thus the costs associated with the incident response will be incurred through acquiring the labour required. Additional costs for the port operators would be the contacting of cargo content owners to inform them of the delays. This would require the establishment of several offices and call centres to process this initial and sustained contact. These costs will be ongoing until port operators have recovered their operational functionality. This coverage typically does not include any public relation costs.

Regulatory and defence

Regulatory and defence loss refers to the regional and federal regulatory costs associated with the cyber event. Within the scenario, Port Operators will face legal challenges, particularly against a spate of new data privacy regulation that has developed in Asia.[67] Port Operators who are fined by regulatory bodies and industry associations will claim on this policy to assist in covering penalties, defence costs, investigations or other regulatory actions.

Reputational damage

The corporate reputation is defined as the perception of a company in the minds of its stakeholders. When an event causes the public's perception of a company to falter long term, they can claim a portion of their losses through a reputational damage policy. In some policies, public relations costs can also be claimed under this coverage. Within the scenario, the business interruption caused by the Shen virus introduces consumer apprehension to international trade. Consumers begin to minimise their reliance on suppliers at large geographical distances, and take steps to source more locally, leading to a reduction in global shipping transaction volumes. The impact is limited, however, as consumers resume their prior habits as the cyber-attack recedes from the societal collective consciousness. The reputational damage is minimal in this scenario due to the geographical significance of ports and their removal from traditional market economy conditions where reputation correlates with business performance.

Data and software

Data and Software loss refers to the cost of lost or damaged electronic data, and the cost of replacement or restoration of data. Within the scenario, the ship manifests are affected, which stores the inventory of the cargo, crew, and passengers on board. The virus later infects Port Operators and Logistics and Cargo Handling Companies, who store information on cargo, inventory, and delivery details. The virus renders the data corrupt or lost and requires reconstituting. In some cases, the software is also damaged by the virus and is required to be rebuilt. The costs associated with this arise from a range of additional activities required that requires outsourcing, such as hiring additional IT Personnel, the legal resources and liabilities that arise from the scenario.

[66] D&O Box: Mooney 2013; Ferguson 2015

[67] Appendix B

Freight, demurrage & defence

Freight, Demurrage & Defence provides coverage for the cost of legal representation in disputes not covered by other insurance policies. The coverage is typically provided in partnership with a Protection and Indemnity (P&I) insurance. Within the scenario, the ships responsible for introducing the virus will likely have substantial demurrage and disputes associated to its arrival. The Freight, Demurrage & Defence policy will support ship owners in their legal costs, and additional legal support. The policy will also support the financing of experts or specialists who are hired to settle the dispute.

Technology Errors and Omissions

Technology Errors and Omissions (Tech E&O) provides liability coverage to providers of technology services and products. Within this scenario, the ship management software and the port management software are found to have been vulnerable to a virus, which manipulates the software and scrambles cargo details. They are deemed partially liable for the extent of loss. The software providers face substantial subrogation lawsuits from insurers impacted by the event.

Contingent Business Interruption

Contingent business interruption (CBI) provides coverage for lost profits or extra expenses occurring due to business interruption of a vendor or client. In the context of cyber, contingent business interruption coverage covers the insured's loss of income and operating expenses due to the disruption of 3rd party digital services and supply chain interruptions.[68]

Within the scenario, shipping suppliers and vendors face business interruption following the closure of the ports and delayed deliveries. Clients dependent on the affected suppliers and vendors faces losses and business interruption due to the supply chain's temporary suspension. A disruption in services and point-of-sale activities are also triggered by the cargo delivery delay. Vendors and clients claim contingent business interruption to recoup their losses.

Theoretically, indirect economic losses could be considerably higher than shown in the report because of the compounding effect of multiple sectoral losses across hundreds of countries and their trading partners at several supply chain tiers. For these losses to match the scale of the report, constraints were placed on the number of countries and supply chain levels modelled. Losses shown still reflect the impact to 155 indirectly affected countries on aggregate. CBI losses are modelled on indirect economic loss using regional insurance penetration rates.

While limits and deductibles are included in the modelling used for this report, CBI sub-limits are not considered.

Analysis of results

The estimated global insurance industry loss ranges from $3.64 – $8.26 billion for the Shen scenario, dependant on the scenario variant. Comparing the insured losses to the economic losses contextualises these results and provides further insights, as shown in Table 9.

Table 9: Overview of the insurance industry losses, $billion

Totals	S1	S2	X1
Insured losses	$3.64	$4.98	$8.29
Economic losses	$40.38	$55.94	$109.86
% of economic losses	8.9%	8.8%	7.5%

An interesting statistic that has been generated is by comparing the insurance industry loss estimates to the economic losses, which provides insight into the insurability of the scenario and potential insurance gaps. In this scenario insurance policies cover 8%-9% of the economic losses, which is slightly lower than catastrophes of a similar scale of economic loss. Most of the insurance coverage is from all risk policies (62%-57%), as demonstrated in Table 10. .

Table 10: Breakdown of insurance industry coverage by type, $billion

Totals	S1	S2	X1
Non- affirmative cyber exposure (All Risks)	$3.64	$4.98	$8.29
% of insurance coverage	*62%*	*61%*	*57%*
Cyber affirmative insured losses	$1.39	$1.94	$3.60
% of insurance coverage	*38%*	*39%*	*43%*

Notably, if this scenario were to occur in a different geography, which had a greater insurance penetration and a more litigious culture, one could anticipate higher economic and insured costs. In an environment such as the United States, there would be greater liability losses across directors and officers, errors and omissions, and general liability, which would significantly compound the losses.

[68] OECD 2017

The insurance gap

This scenario presents a substantial insurance gap, leaving about 92% of the losses un-insured. The losses are likely to be felt across the marine trading industry, and ripple across various interconnected networks. The reasoning for the gap is multi-faceted and is the responsibility of insurers and clients alike, requiring joint investment to respond effectively.

From a marine insurance perspective, many traditional policies exclude cyber and non-physical events. Accordingly, events which do not result in physical damage can be difficult to claim. Within the scenario, this was most clearly seen in the gap between the insured cargo and the total cargo affected. Current cargo BI policies exclude delay, unless the cargo has been physically damaged. Within this scenario, this is limited to the 7% of the cargo which has temperature sensitive materials spoiled due to the delay. In the future, policies should continue to evolve and offer more cyber write backs and cyber-affirmative policies.

Another contributor to the gap was the limits available for cyber events, specifically seen in Cyber Affirmative Policies. The limits were frequently unable to support the scale of losses which were projected to occur in this scenario. Cyber Insurance policies should continue to adapt their limits and policy structures to account for the scale of potential losses.

From a client perspective, there remains limited insurance penetration in Asia, compared to what is seen in other jurisdictions. There is still a large number of corporates who are not purchasing sufficient insurance, whether for liability or cyber risks. Notably, many are still choosing policies which do not account for cyber risks or similar write backs, or do not purchase sufficient cover and high enough limits. As risks become more expensive and interconnected, clients must proactively purchase insurance to protect themselves and their business.

Conclusions

7. Conclusions

This report deepens insurers' and risk managers' understanding of cyber-risk liability and aggregation. It shows the vital contribution research and analysis can make in reducing uncertainty concerning cyber risk.

This scenario emphasises to organisations – individual entities, industry associations, markets and policy makers – the importance of raising awareness of the risk, assessing the potential damage it could cause through very large and complex global supply chain.

The projected growth of connectivity and connected devices in the next decade has the potential for increased growth in the maritime sector, but this growth will come hand-in-hand with increased risk if not managed appropriately. Global hyper connectivity has the potential to quickly turn isolated cyber events into global cyber catastrophes as seen in the Shen narrative.

The Shen scenario was crafted to highlight the current potential for loss in unchecked supply chains and the far-reaching nature of these losses in years to come. The economic losses in the Shen scenario are driven by the number of countries affected, the number of ports affected, and the amount of time each port is shut down for. Container terminals are crucial for imports and exports for a wide range of sectors, including Transportation, Manufacturing, Retail, and Business & Professional Services. A cyber-attack on ports has the potential to significantly restrict the operations of all of these sectors simultaneously, often for multiple countries.

From an insurance perspective, the Shen scenario reveals a significant insurance gap in the Asia-Pacific region due to the low levels of insurance penetration - approximately 92% of losses in the scenario are uninsured. This presents both a risk and an opportunity for businesses, investors, and insurers, who can choose to improve insurance take-up rates in the region, particularly to benefit the marine trading industry.

Future developments to this work may take the form of more extensive modelling that considers a wider range of macro-economic variables and delves deeper into the geographic interplay between countries' transportation networks and trade routes. Technology is always changing. Updates may include reassessments of the technology underpinning port management systems and widely used by ships and ship management companies, and how these networks are interlinked.

This report was intended to be a thought-provoking piece. Hypothetical, deterministic scenarios provide a test bed for businesses, analysts, insurers, and economists to get a sense of looming threats to their business and the ensuing financial fallouts without suffering the losses. The events detailed here and in other scenario reports are low probability, high impact events. They are not meant to be a definitive forecast of events to come.

There are lessons for the insurance sector, too, as the report also highlights potential insurance policy, legal, and aggregation issues in cyber insurance offerings. To address them data collection and quality is important, especially as cyber risks are constantly changing.

Drivers of losses

In the scenario and its variants, there are several key aspects contributing to losses:

1. The number of ports within a country
   Though ports are similar in many fundamental ways, such as operations and personnel, they can differ widely in terms of cargo types, freight statistics, ship and cargo monitoring, operational technologies, and geographical considerations. For some of the countries affected by the Shen attack, the effects will ripple through the supply chain to hundreds of minor ports in the country.

2. Port efficiency
   Port efficiency incorporates information on business subscription, the size of vessels that can be accommodated within a port, and the technical efficiency with which cargo is received and released from ports. The better the efficiency of a port, the less downtime they will experience in an event such as this. TEU throughput is also a standard measure of productivity for a port.

3. Port connectivity
The interdependent and complex nature of maritime supply chains is well documented. The annual liner shipping connectivity index considers the number of companies that deploy container ships on services to and from a country's ports combined with other measurements to capture the country's level of integration into the liner shipping network and trade facilitation.

4. Surrounding area
The GDP of neighbouring countries may impact the cargo throughput of the affected ports because the cargo throughput of geographically near ports are dependent on each other. This is in part due to transhipments, where goods are shipped to intermediate destinations before reaching their final port. An increased ability to handle transhipping operations at neighbouring ports combined with an increase in cargo throughput at the destination ports leads to this interdependency, making GDP an important determinant of container throughput.
In the event of a severe cyber-attack, ships will be rerouted to nearby ports where possible but, for some countries surrounded by countries with a lower GDP, this will have limited efficiency and possibly slow recovery.

Insurance opportunities

There are also opportunities for insurers to grow their business in the insurance classes associated with the Shen Attack scenario. For example, Asia is one of the fastest-growing markets for cyber insurance. The market saw an 87% increase in cyber insurance take-up rates in Asia in 2017 with the current global premiums estimated to total $50 million.[69]

The increase in cyber-attacks in 2017 in Asia over recent years means companies are more likely to have standalone cyber insurance than before, although with low sub-limits and more limited take-up of first party BI coverage when compared to other markets. Further insurance take-up is likely in the future for directors and officers (D&O) policies as changes in the business environment as such tight corporate governance and new regulations are introduced. Finally, systemic cyber vulnerabilities can have a catastrophic effect on the global supply chain, stemming from the directly affected country or sector with contingent business interruption identified as particularly damaging.

CyRiM research

The 'Shen attack: Cyber risk in Asia Pacific ports' and the 'Bashe Attack: Global infection by contagious malware' are two joint reports produced by the Cyber Risk Management (CyRiM) project led by Nanyang Technological University, Singapore in collaboration with industry partners and academic experts including the Cambridge Centre for Risk Studies. CyRiM industry founding members include Aon, Lloyd's - the specialist insurance and reinsurance market, MSIG, SCOR and TransRe. These scenarios will help policyholders and insurers to expand their view of cyber risks ahead of the next event and help them, create new products and services that can make businesses and communities more resilient.

[69] Williams 2016; Weinland 2017; OECD 2017

References

Aon Risk Solutions. n.d. “Client Alert: WannaCry Cyber Attack.” http://www.aon.com/attachments/risk-services/cyber/Client-Alert-WannaCry-Cyber-Attack.pdf.

Asia Briefing, Dezan Shira & Associates. 2019. “China’s Cybersecurity Law.” Asia Briefing, Dezan Shira & Associates. https://www.dezshira.com/library/legal/cyber-security-law-china-8013.html.

Bailey, Rob, and Laura Wellesley. 2017. “Chokepoints and Vulnerabilities in Global Food Trade.” Chatham House - The Royal Institute of International Affairs - Energy, Environment and Resources Department. https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-27-chokepoints-vulnerabilities-global-food-trade-bailey-wellesley.pdf.

Banner, Simon. 2019. “England & Wales: IUA Publishes Two New Model Cyber Exclusions | Lexology.” June 13, 2019. https://www.lexology.com/library/detail.aspx?g=6dff4159-b703-4ebb-8c31-7e00124755fa.

Basta, Nicholas. 2018. “The 2018 Pharma Cold Chain: More Data Leads to Less Risk.” Pharmaceutical Commerce. September 3, 2018. https://pharmaceuticalcommerce.com/cold-chain-focus/the-2018-pharma-cold-chain-more-data-leads-to-less-risk/.

Baxter, Michael. 2018. “Data Backup and Blockchain, Is This a Game Changer?” Information Age (blog). December 6, 2018. https://www.information-age.com/data-backup-and-blockchain-123477187/.

Bhattacharjee, Shilavadra. 2011. “What Is Electronic Chart Display and Information System (ECDIS)?” Marine Insight (blog). January 18, 2011. https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/.

———. 2017. “Automatic Identification System (AIS): Integrating and Identifying Marine Communication Channels.” Marine Insight (blog). March 27, 2017. https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/.

Buck, Graham. 2018. “Expanding Cyber BI.” Risk & Insurance. March 5, 2018. http://riskandinsurance.com/expanding-cyber-bi/.

Burnson, Patrick. 2015. “Defining Threats and Finding Solutions for Cyber Attacks.” June 9, 2015. https://www.scmr.com/article/defining_threats_and_finding_solutions_for_cyber_attacks.

Cambridge Centre for Risk Studies, Lloyd’s of London, and Nanyang Technological University. 2019. “Bashe Attack: Global Infection by Contagious Malware.” https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/space-and-technology/cyrim-scenario-bashe-attack/.

CargoChain. 2019. “Partners - CargoChain.” 2019. https://www.cargochain.com/partners.

CCRS. 2018. “Multi-Line Insurance Exposure Management Data Definitions Document v1.0.” 2018. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-geac-data-definitions-document.pdf.

Centre for the Straits of Malacca (CSOM). 2018. “Centre for the Straits of Malacca (CSOM).” MIMA | Maritime Institute of Malaysia. 2018. http://www.mima.gov.my/research/the-straits-of-malacca-csom/csom-introduction.

“China Merchants Holdings (International) Company Limited (CMHI) - Organizations - China CSR Map.” n.d. Accessed March 1, 2019. http://www.chinacsrmap.org/Org_Show_EN.asp?ID=1340.

Choi, Seung Soo, and Seungmin Jasmine Jung. 2018. “Korea: Cybersecurity 2019.” Text. International Comparative Legal Guides International Business Reports. October 16, 2018. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/korea.

CNN. 2011. “Australia’s Expensive Bananas | CNN Travel.” August 8, 2011. ./.

Controlant. 2018. “The emergence of ocean freight for pharmaceutical supply chain logistics.” Controlant. April 3, 2018. http://controlant.com/blog/2018/the-emergence-of-ocean-freight-for-pharmaceutical-supply-chain-logistics/.

Cruise Port Guide of Japan. 2014. “Port of Kitakyushu (Moji, Hibiki).” Mlit.Go.Jp. 2014. http://www.mlit.go.jp/kankocho/cruise/detail/054/index.html.

"Cyber – Clause 380 Buy-Back." 2017. Norwegian Hull Club. April 25, 2017. https://www.norclub.com/products/special-risks/cyber-clause-380-buy-back-/.

Cyber Security Agency of Singapore. 2019. "Cybersecurity Act." January 17, 2019. www.csa.gov.sg/legislation/cybersecurity-act.

CyberKeel. 2014. "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas." Copenhagen, Denmark. https://docplayer.net/19421672-Maritime-cyber-risks-virtual-pirates-at-large-on-the-cyber-seas-10-15-2014.html.

CyberSecurity Malaysia. n.d. "CyberSecurity Malaysia." CyberSecurity Malaysia. Accessed June 11, 2019. http://www.cybersecurity.my/en/media_centre/media_faqs/media_faqs/main/detail/1691/index.html.

"Efficiency of World Ports in Container and Bulk Cargo (Oil, Coal, Ores and Grain)." 2012. OECD Regional Development Working Papers 2012/09. https://doi.org/10.1787/5k92vgw39zs2-en.

European Global Navigation Satellite Systems Agency. 2016. "What Is GNSS?" March 1, 2016. https://www.gsa.europa.eu/european-gnss/what-gnss.

Fairplay IHS. 2017. "Hanjin Shipping Declared Bankrupt, Ending 40-Year Existence." Fairplay IHS. February 17, 2017. https://fairplay.ihs.com/commerce/article/4282281/hanjin-shipping-declared-bankrupt-ending-40-year-existence.

Ferguson, Nick. 2015. "D&O Still a Tough Sell in Asia." InsuranceAsia News (blog). July 17, 2015. https://insuranceasianews.com/do-still-a-tough-sell-in-asia/.

Geocoops. n.d. "Population Density Distribution in Japan." http://www.geocoops.com/uploads/2/4/5/3/24532387/fs_-_population_density__distribution_in_japan.pdf.

Government of the Republic of Korea. 2009. "Act on Promotion of Information and Communication Network Utilization and Information Protection." Wikisource. https://en.wikisource.org/wiki/Act_on_Promotion_of_Information_and_Communication_Network_Utilization_and_Information_Protection.

Gritsi, Eliza. 2019. "Dust Has yet to Settle Two Years after China's Landmark Cybersecurity Law." TechNode (blog). June 10, 2019. https://technode.com/2019/06/10/dust-has-yet-to-settle-two-years-after-chinas-landmark-cybersecurity-law/.

Hall, Peter V. 2004. "'We'd Have to Sink the Ships': Impact Studies and the 2002 West Coast Port Lockout." Economic Development Quarterly 18 (4): 354–67. https://doi.org/10.1177/0891242404269500.

HarvardCID. 2016. "The Atlas of Economic Complexity." Atlas of Economic Complexity. 2016. http://atlas.cid.harvard.edu/explore/?country=192&partner=43&product=undefined&productClass=HS&startYear=undefined&target=Partner&year=2016.

Hayashi, Hiromi. 2018. "International Comparative Legal Guides." International Comparative Legal Guides International Business Reports. October 16, 2018. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/japan.

Hellenic Shipping News. 2017. "Japan's Maritime Technology Roadmap to 2050." November 24, 2017. https://www.hellenicshippingnews.com/japans-maritime-technology-roadmap-to-2050/.

Hill, Rebecca. 2018. "Great. Global Internet Freedoms Take Another Dive as Censorship and Fake News Proliferate." The Register. November 2, 2018. https://www.theregister.co.uk/2018/11/02/internet_freedom_report_2018/.

"How Many Islands Are There in Japan?" n.d. Japan Talk. Accessed March 1, 2019. https://www.japan-talk.com/jt/new/how-many-islands-are-there-in-Japan.

IMO. 2019. "International Maritime Organisation." 2019. https://business.un.org/en/entities/13.

Insurance Journal. 2019. "Beazley Launches Affirmative Marine Cyber Cover." Insurance Journal. May 15, 2019. https://www.insurancejournal.com/news/international/2019/05/15/526480.htm.

International Maritime Organization (IMO). 2017. "Guidelines on Maritime Cyber Risk Management." International Maritime Organization (IMO). http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Guidance/Documents/MSC-FAL.1-Circ.3.pdf.

———. 2018. "Adoption of the Initial IMO Strategy on Reduction of GHG Emissions from Ships and Existing IMP Activity Related to Reducing GHG Emissions in the Shipping Sector." International Maritime Organization (IMO). https://unfccc.int/sites/default/files/resource/250_IMO%20submission_Talanoa%20Dialogue_April%202018.pdf.

JLT. 2018. "Cyber Drives Business Interruption Concerns." March 1, 2018. http://www.jltspecialty.com/our-insights/publications/cyber-decoder/cyber-drives-business-interruption-concerns.

Kuok Ho, Daniel Tang. 2018. "Climate Change in Malaysia: Trends, Contributors, Impacts, Mitigation and Adaptations." Science of The Total Environment, September. https://doi.org/10.1016/j.scitotenv.2018.09.316.

Lloyd's. 2018a. "One Hundred Container Ports 2018." Lloyd's List. 2018. https://lloydslist.maritimeintelligence.informa.com/one-hundred-container-ports-2018.

———. 2018b. "Top 10 Shipmanagers 2018." Lloyd's List Maritime Intelligence Informa. December 7, 2018. Top 10 shipmanagers 2018.

Lloyd's List. 2017. "One Hundred Ports." 2017. https://sdwerecruit.co.uk/wp-content/uploads/2017/10/Lloyds-List-Top-100-Ports-2017-Report.pdf.

Loh, Hui Shan, and Vinh Van Thai. 2015. "Cost Consequences of a Port-Related Supply Chain Disruption." The Asian Journal of Shipping and Logistics 31 (3): 319–40. https://doi.org/10.1016/j.ajsl.2015.09.001.

Malynn, Kelly. 2019. "Cyber Defence for Marine." Beazley. 2019. https://www.beazley.com/.

Marine Insight. 2017. "Photo of AIS." Marine Insight (blog). March 27, 2017. https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/.

Marine Traffic. 2019. "Global Ship Tracking Intelligence." May 30, 2019. https://www.marinetraffic.com/en/ais/home/centerx:107.3/centery:20.7/zoom:4.

Martin Dingeldey, Philipp. 2017. "Port Automation and Cybersecurity Risks." The Maritime Executive. December 22, 2017. https://www.maritime-executive.com/editorials/port-automation-and-cybersecurity-risks.

Ministry of Transport Malaysia. 2017. "Statistik Pengangkutan Malaysia - Transport Statistics Malaysia." Ministry of Transport Malaysia. http://www.mot.gov.my/en/Statistik%20Tahunan%20Pengangkutan/Transport%20Statistic%20Malaysia%202017.pdf.

Mooney, Sean. 2013. "Managing the Rise of D&O Insurance Demand in Asia." Global Reinsurance. November 18, 2013. https://www.globalreinsurance.com/managing-the-rise-of-dando-insurance-demand-in-asia/1405712.article.

MPA Singapore. 2019. "Facts and Trivia." MPA.Gov.Sg. 2019. https://www.mpa.gov.sg/web/portal/home/maritime-singapore/introduction-to-maritime-singapore/facts-and-trivia.

Murphy, Jessica. 2018. "Will Global Warming Open up Arctic Trade?," November 1, 2018, sec. Business. https://www.bbc.com/news/business-45527531.

Navis. 2018. "Trends for Shipping Industry in 2019." December 13, 2018. https://safety4sea.com/navis-trends-for-shipping-industry-in-2019/.

Nayoga Port Terminal Corporation. 2012. "The First Automated Container Terminal in Japan." Nayoga Port Terminal Corporation. 2012. http://www.nptc.co.jp/en/container/automatedct.html.

News24. 2015. "Calais Strike Clogs UK Road with 3000 Trucks." News24. July 1, 2015. https://www.news24.com/World/News/Calais-strike-clogs-UK-road-with-3-000-trucks-20150701.

Ocean Insights. 2018. "ONE: Japan's K-Line, MOL, NYK to Merge Container Shipping Business." Ocean Insights (blog). February 2, 2018. https://www.ocean-insights.com/liner-news/ocean-network-express/.

OEC. 2017. "Japan (JPN) Exports, Imports, and Trade Partners." The Observatory of Economic Complexity. 2017. https://atlas.media.mit.edu/en/profile/country/jpn/.

OECD. 2015. "Input-Output Tables." OECD. 2015. https://stats.oecd.org/Index.aspx?DataSetCode=IOTS.

———. 2017. "Enhancing the Role of Insurance in Cyber Risk Management." OECD Publishing, Paris, 142. http://dx.doi.org/10.1787/9789264282148-en.

Outsourcing Pharma. 2017. "The Move from Cold-Chain to Temperature-Controlled Shipping." Outsourcing-Pharma.Com. June 8, 2017. https://www.outsourcing-pharma.com/Headlines/Promotional-Features/Temperature-controlled-pharmaceutical-logistics.

Paris, Costas. 2018. "Japan's Top Container Shipping Line Sees Loss." MarketWatch. October 16, 2018. https://www.marketwatch.com/story/japans-top-container-shipping-line-sees-loss-2018-10-16.

"Perishable Cargo Handling." 2019. Golden International Logistics Group. 2019. http://goldenlogisticskwt.com/perishable-cargo-handling/.

"Petya Cyber Industry Loss Passes $3bn Driven by Merck & Silent Cyber: PCS - Reinsurance News." 2018. ReinsuranceNe.Ws (blog). November 7, 2018. https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/.

Pharmaceutical Commerce. 2018. "The 2018 Market for Pharma Cold Chain Logistics Is $15 Billion." Pharmaceutical Commerce. May 8, 2018. https://pharmaceuticalcommerce.com/clinical-operations/the-2018-market-for-pharma-cold-chain-logistics-is-15-billion/.

Pillai, Deepak, and Yong Shih Han. 2018. "Malaysia: Cybersecurity 2019." International Comparative Legal Guides International Business Reports. October 16, 2018. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/malaysia.

Port Shanghai. 2018a. "Port Shanghai - Integrated Innovative Technologies Used in the Terminal Construction." 2018. http://www.portshanghai.com.cn/en/channel5/channel51.html.

———. 2018b. "Port Shanghai - Tally Wireless Control System." Port Shanghai. 2018. http://www.portshanghai.com.cn/en/channel5/channel53.html.

———. 2018c. "Port Shanghai - Unmanned Automatic Container Yard." Port Shanghai. 2018. http://www.portshanghai.com.cn/en/channel5/channel54.html.

Port Technology. 2018a. “Automated Container Terminal Market to Hit $10.89 Billion.” Port Technology. May 2, 2018. https://www.porttechnology.org/news/automated_container_terminal_market_to_hit_10.89_billion.

———. 2018b. “South Korea Pilots Blockchain in Busan.” Port Technology. December 19, 2018. https://www.porttechnology.org/news/south_korea_pilots_blockchain_in_busan.

Reed Smith. 2018. “China’s Cybersecurity Law.” Reed Smith. https://www.reedsmith.com/-/media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf.

Rose, Adam, and Dan Wei. 2013. “Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience.” Economic Systems Research 25 (2): 212–32. https://doi.org/10.1080/09535314.2012.731379.

SG Maritime. 2018. “Ship Management.” Sgmaritime.Com. 2018. https://www.sgmaritime.com/categories/ship-management.

Ship Technology. 2019. “Port of Shanghai.” Ship Technology (blog). 2019. https://www.ship-technology.com/projects/portofshnaghai/.

Sims, David. 2013. “China Widens Lead as World’s Largest Manufacturer.” March 14, 2013. https://news.thomasnet.com/imt/2013/03/14/china-widens-lead-as-worlds-largest-manufacturer.

Singapore Statutes Online. 2018. “Cybersecurity Act 2018.” Singapore Statutes Online. 2018. https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312.

Son, Doil, and Sun Hee Kim. 2019. “Korea Cybersecurity.” Getting The Deal Through. February 2019. https://gettingthedealthrough.com/.

Songbing, Ding. n.d. “Shanghai Port: Yangtze Growth Strategy | Port Technology.” Port Technology. Accessed February 7, 2019. https://www.porttechnology.org/technical_papers/shanghai_port_yangtze_growth_strategy.

Statista. 2018. “Container Shipping - Statistics & Facts.” October 10, 2018. https://www.statista.com/topics/1367/container-shipping/.

Stratfor. 2012. “Japan’s Maritime Strategy.” Worldview Stratfor. June 26, 2012. https://worldview.stratfor.com/article/japans-maritime-strategy.

Tam, Kimberly, and Kevin D. Jones. 2018. “Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping.” Journal of Cyber Policy 3 (2): 147–64. https://doi.org/10.1080/23738871.2018.1513053.

The Maritime Executive. 2019. “Singapore’s Port Authority Opens New Cybersecurity Center.” The Maritime Executive. May 16, 2019. https://www.maritime-executive.com/article/singapore-s-port-authority-opens-new-cybersecurity-center.

The Observatory of Economic Complexity. 2017. “Products Exported by China 2017.” The Observatory of Economic Complexity. 2017. http://atlas.media.mit.edu/en/visualize/tree_map/hs92/export/chn/all/show/2017/.

The Security Ledger. 2017. “NotPetya Infection Left Merck Short of Key HPV Vaccine.” The Security Ledger. October 27, 2017. https://securityledger.com/2017/10/notpetya-infection-left-merck-short-key-vaccine-gardasil/.

The World Bank. 2017. “GDP (Current US$) | Data.” The World Bank. 2017. https://data.worldbank.org/indicator/ny.gdp.mktp.cd.

Trading Economics. 2019. “South Korea Imports.” Trading Economics. 2019. https://tradingeconomics.com/south-korea/imports.

Transport Geography. 2017. “Liner Shipping Connectivity Index and Container Port Throughput.” The Geography of Transport Systems (blog). November 8, 2017. https://transportgeography.org/?page_id=2078.

UKHO. 2016. “ECDIS Photo.” SAFETY4SEA (blog). October 21, 2016. https://safety4sea.com/risks-paperless-chart-systems-incidents-due-ecdis-improper-use/.

UNCTAD. 2017. “UNCTADstat - Maritime Profiles.” UNCTADstat. 2017. https://unctadstat.unctad.org/CountryProfile/MaritimeProfile/en-GB/251/index.html.

———. 2018. “Review of Maritime Transport 2018,” 116.

UNCTADstat. 2018a. “Liner Shipping Bilateral Connectivity Index, Annual.” 2018. https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=96618.

———. 2018b. “Liner Shipping Connectivity Index, Annual.” UNCTADstat. 2018. https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=92.

U.S. Energy Information Administration (EIA). 2017. “The Strait of Malacca, a Key Oil Trade Chokepoint, Links the Indian and Pacific Oceans.” August 11, 2017. https://www.eia.gov/todayinenergy/detail.php?id=32452.

Wagner, Jack. 2017. “China’s Cybersecurity Law: What You Need to Know.” The Diplomat. June 1, 2017. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

Wang, Xiaolin. 2014. “The Impact of Economic Crisis on Ports in Post-Crisis Period: A Study on Cargo Throughput in Hamburg-Le Havre Range.” Erasmus University Rotterdam. https://thesis.eur.nl/pub/16633/MA-thesis-Y.Wang.pdf.

WCN Editorial. 2018. “Jade Logistics Makes a Blockchain Move.” WorldCargo News. September 13, 2018. https://www.worldcargonews.com/news/news/jade-logistics-makes-a-blockchain-move-60614.

Weinland, Don. 2017. “AIG Reports 87% Rise in Asia Cyber Insurance Requests.” Financial Times, August 9, 2017. https://www.ft.com/content/6362bc1a-2af4-3442-b461-f679174bc72d.

Wikipedia. 2017a. “Port of Mokpo.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=Port_of_Mokpo&oldid=779111520.

———. 2017b. “Shen (Clam-Monster).” In Wikipedia. https://en.wikipedia.org/w/index.php?title=Shen_(clam-monster)&oldid=814121054.

———. 2018a. “Port of Nagoya.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=Port_of_Nagoya&oldid=832976345.

———. 2018b. “Port of Shanghai.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=Port_of_Shanghai&oldid=868396287.

———. 2018c. “List of Busiest Ports by Cargo Tonnage.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=List_of_busiest_ports_by_cargo_tonnage&oldid=874749998.

———. 2018d. “Port of Busan.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=Port_of_Busan&oldid=874781066.

———. 2019. “China Internet Security Law - Controversies.” In Wikipedia. https://en.wikipedia.org/w/index.php?title=China_Internet_Security_Law&oldid=898768498.

Williams, Ann. 2016. “Demand for Cyber Insurance in Singapore to Grow by 50% in 2016: AIG.” The Straits Times, March 31, 2016. http://www.straitstimes.com/business/banking/demand-for-cyber-insurance-in-singapore-to-grow-by-50-in-2016-aig.

World Atlas. 2018. “City Populations, Largest Cities of the World.” World Atlas. 2018. https://www.worldatlas.com/citypops.htm.

World Integrated Trade Solution. 2017. “Trade at a Glance: Most Recent Values.” World Integrated Trade Solution. 2017. https://wits.worldbank.org/countrysnapshot/en/CHN.

World Maritime News. 2017. “In Depth: Smart Ships Are Coming!” April 24, 2017. https://worldmaritimenews.com/archives/218365/interview-smart-ships-are-coming/.

World Port Source. 2019a. “Port of Busan.” World Port Source. 2019. http://www.worldportsource.com/ports/review/KOR_Port_of_Busan_1482.php.

———. 2019b. “WPS - Map of Ports in China.” World Port Source. 2019. http://www.worldportsource.com/ports/CHN.php.

World Shipping Council. n.d. “Trade Statistics | World Shipping Council.” Accessed September 12, 2018. http://www.worldshipping.org/about-the-industry/global-trade/trade-statistics.

Wuerthele, Mike. 2017. “Apple, Other Companies Pull Skype from Chinese App Stores at Request of Government.” AppleInsider. November 21, 2017. https://appleinsider.com/articles/17/11/21/apple-other-companies-pull-skype-from-chinese-app-stores-at-request-of-government.

Yahoo! Finance. 2018. “China’s Cybersecurity Law Isn’t Just About Cybersecurity.” Yahoo! Finance. January 29, 2018. https://finance.yahoo.com/news/china-cybersecurity-law-isn-t-061354139.html.

Yik, Chia Swee. 2018. “Basics of Cyber Security Law in Malaysia.” Chialee. October 25, 2018. http://www.chialee.com.my/knowledge-hub/basics-of-cyber-security-law-in-malaysia/.

Appendix A: Maritime profiles of directly impacted countries

A brief overview of the maritime profiles of the countries directly impacted by the Shen Attack Scenario.

Japan

Japan is a maritime power out of necessity, as the island nation encompasses four major islands and approximately 6,800 minor ones,[70] covering a substantial area. Seaborne trade grew out of this maritime strength, making Japan one of the largest exporters in the world. Major exports include cars and vehicle parts, integrated circuits, and machinery, while it primarily imports crude petroleum, petroleum gas, and broadcasting equipment.[71] The main trade partners receiving those exports are China and the United States of America.

The largest and busiest port in Japan is the port of Nagoya, accounting for 10% of Japan's total trade value. Toyota exports most of its cars through this port, making Nagoya the largest vehicle exporter in the country.[72] The port boasts the first automated container terminal in Japan, allowing the reception of incoming containers through a gate that channels the heavy-haul trucks into designated lanes via a remote operating room.

Once in the appropriate lane, containers are transferred to storage or cargo ships with rubber tyred gantry (RTG) cranes. The whole process in the storage area is automated whereas the cargo-handling area relies on remote manual operation, with one driver controlling multiple RTGs.[73] This is an important advance in a market where automated container terminals are expected to grow to nearly $11 billion in 2023.[74]

In 2017, the National Maritime Research Institute of Japan presented their 2050 roadmap for science and technology in shipping, including some game-changing innovations in the fields of self-healing materials, 3D printing, autonomous or uncrewed ships, robotics, and big data analysis of logistics data.[75]

Three of Japan's biggest container shipping lines invested $3 billion[76] to merge their companies in 2018. Kawasaki Kisen Kaisha (K Line), Nippon Yusen Kabushiki Kaisha (NYK), and Mitsui O.S.K. (MOL) now jointly operate the Ocean Network Express (ONE). This merger makes ONE the sixth biggest company in terms of vessel capacity globally.[77]

[70] Stratfor 2012
[71] OEC 2017
[72] Wikipedia 2018a
[73] Nayoga Port Terminal Corporation 2012
[74] Port Technology 2018a
[75] Hellenic Shipping News 2017
[76] Paris 2018
[77] Ocean Insights 2018

Malaysia

The Straits of Malacca to the west of Malaysia is one of the most important international waterways in the world, connecting the Indian and Pacific Oceans and major Asia-Pacific economies since the 7th Century.[78] The second-largest oil trade chokepoint in the world, one-third of global petroleum transported on maritime routes passed through the Strait of Malacca in 2015. A blockage to the Strait would cause nearly half of the world's ships to reroute around the Indonesian archipelago, tying up global shipping capacity and affecting energy prices. The addition of a natural gas pipeline between Myanmar and China in August 2014 has allowed for a reduction in critical tanker traffic through the Strait.[79]

Figure 28: Indian Ocean to Pacific Ocean maritime chokepoint

Kelang Port on the west coast is the largest container port by handling of export and imports, moving nearly 12 million TEUs in 2017.[80] Because of its location, transhipments are a major part of the movement of goods through the Malaysia ports, accounting for a third of total cargo throughput by tonnage in 2017.[81]

Malaysia is already feeling the effects of climate change,[82] prompting the International Maritime Organisation's Marine Environment Protection Committee to adopt a strategy in 2018 to reduce greenhouse gas emissions from international shipping with the goal to phase them out entirely within the century. These reduction efforts are in line with the Paris Climate Agreement and the UN's Sustainable Development Goals.[83]

[78] Centre for the Straits of Malacca (CSOM) 2018
[79] U.S. Energy Information Administration (EIA) 2017
[80] Ministry of Transport Malaysia 2017
[81] Ministry of Transport Malaysia 2017
[82] Kuok Ho 2018
[83] International Maritime Organization (IMO) 2018

Singapore

Maritime trade has served as a critical lifeline for Singapore since it was founded in 1819. The Singapore port serves as a connection hub to all of Asia and has strong connections to 120 countries and 600 ports. These are important commercial ties in a world where 90% of the world's trade is carried by sea, which is the most environmentally friendly and energy-efficient method of cargo transport.[84] The Singapore port is the third-busiest in terms of tonnage handled.[85]

1,000 vessels are docked at the Singapore port at any one time, with a ship arriving or leaving every 2-3 minutes. The Maritime and Port Authority's Port Operations Control Centre monitors all vessels passing through the Singapore Strait, tracking up to 10,000 vessels at a time. Presently, the Singapore Registry of Ships has over 4,500 vessels registered with it, making it one of the top 5 largest ship registries globally.[86]

Singapore is the top ship refuelling (or bunkering) port in the world, though the country does not produce any oil itself. In terms of maritime establishments, more than 5,000 organisations are involved, contributing 7% to Singapore's GDP and responsible for 170,000 jobs.[87]

Box 8: New mega port in development

Singapore is developing a new fully-automated port called the Tuas Mega Port, heralded as the next generation of container management and port modernisation. It is set to open in 2021. By 2040, it will have capacity for 65 million twenty-foot equivalent units of cargo annually, making it one of the largest ports in the world.

The automated terminal will primarily assist with storage planning, which offers many operational benefits. However, the automation also increases cyber risk vulnerability because of the networked systems.

The Republic of Korea

The Republic of Korea's primary imports are petroleum products, machinery, and appliances.[88] Its maritime industry suffered in early 2017 when Hanjin Shipping, a 40-year-old institution with over $5 billion debt, was declared bankrupt. Hanjin's container terminals had struggled with chronic overcapacity, and its liquidation caused logistical chaos as vessels were stranded all over the world and creditors sought out the ships. In 2018, Seoul announced a five-year plan to steer The Republic of Korea's maritime industry in a more profitable direction, aiming to generate $45 billion in revenue by 2022.[89]

The Port of Busan in The Republic of Korea is uniquely located just 203 kms from the Port of Kitakyushu in Japan, roughly in the centre of North-Eastern Asia,[90] and 247 kms from The Republic of Korea's Port of Mokpo,[91] a major port in the Yellow Sea.[92] The port is a metropolitan city under direct control by the central government, effectively giving it the status of a province. It is home to major industries including steel, ceramics, chemicals, shipbuilding, automobiles, and electronics, with new industrial parks bringing in high-tech manufacturers.

The Port of Busan is the largest port in The Republic of Korea, the tenth busiest port in Northeast Asia, and the fifth busiest container port in the world.[93] Its top exports include cars, vehicle parts, refined petroleum, and integrated circuits. The country primarily exports to China, the United States, Vietnam, Hong Kong Special Administrative Region of the People's Republic of China, and Japan, with imports coming from a range of countries including Germany and other Asian countries.[94]

Box 9: Blockchain

The Republic of Korean government announced in December 2018 that they intend to launch a blockchain pilot project in the Port of Busan to improve efficiencies at an initial cost of $9 million. The goal is to see if the supply chain can be made more transparent and if this will quicken the administration process using real-time data sharing. If successful, the project will be rolled out to other ports in the country. The blockchain will improve livestock record management, international document distribution, and customs clearance, in addition to shipping logistics.

[84] Box "New Mega Port in Development": Martin Dingeldey 2017
[85] Wikipedia 2018b
[86] MPA Singapore 2019
[87] MPA Singapore 2019
[88] Trading Economics 2019
[89] Fairplay IHS 2017
[90] Cruise Port Guide of Japan 2014
[91] World Port Source 2019
[92] Wikipedia 2017
[93] Box "Blockchain Pilot": Port Technology 2018
[94] Wikipedia 2018c

China

China is one of the world's largest maritime countries. It is one of the oldest and most important industries in a country with a coastline of over 14,000 km.

Though China has hundreds of ports,[95] the largest is the port of Shanghai located at the mouth of the Yangtze River, covering an area of 3,619km^2.

It dates back to the fifth century, opening for international trade in the mid-1800s.[96] Public terminals at the port are managed by the Shanghai International Port Group, a publicly listed company predominantly owned by the Municipal Government. The Shanghai port is an important entry and exit point for foreign trade, serving dense population areas with strong industrial and agricultural sectors.[97] Shanghai is the third largest city in the world in terms of population (over 24 million).[98] The Yangtze Economic Zone contributes over 40% of China's GDP and is responsible for 25% of China's cargo imports and exports.[99]

Terminals at the Shanghai port have developed at unprecedented speeds, proving to be a marvel of the maritime industry. With this growth has come innovative technologies, such as the installation of an unstaffed automatic container yard. The digitised intelligent port system has an autonomous stacking technique that allows for a stack eight containers high, nearly double the world average, utilising the available space more efficiently.[100] The port also has a wireless handheld control system for tallying containers at terminals,[101] and a range of engineering advances related to land reclamation.[102]

Figure 29: Ports in China (port of Shanghai in purple)

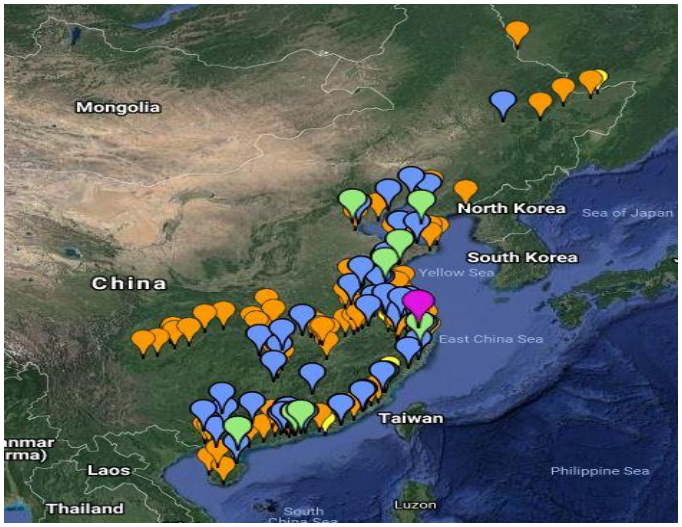
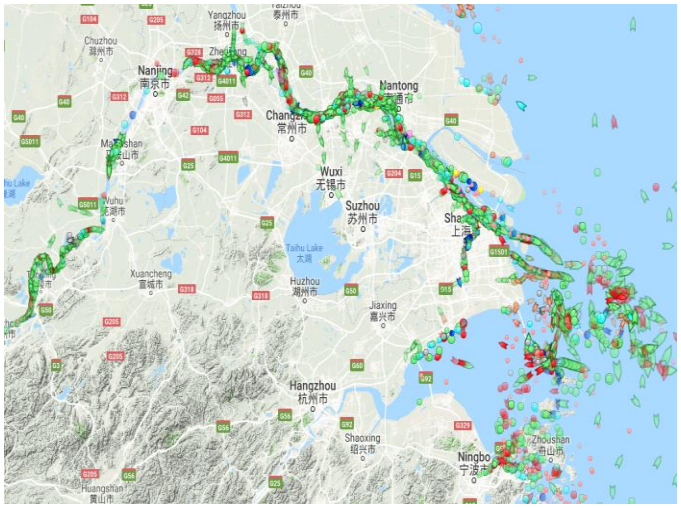


Figure 30: Heavy sea traffic on the Yangtze River near the Shanghai Port and Ningbo-Zhoushan Port, China



[95] World Port Source 2019b
[96] Ship Technology 2019
[97] Wikipedia 2018a
[98] World Atlas 2018
[99] Songbing n.d.
[100] Port Shanghai 2018c
[101] Port Shanghai 2018b
[102] Port Shanghai 2018a

Appendix B: Cyber security regulations in directed impacted countries

An overview of the cyber security regulations in the directly impacted countries in the Shen attack scenario.

Japan

The key regulation governing cybersecurity in Japan is the Act on the Prohibition of Unauthorised Computer Access (the UCAL), supported by the national Penal Code. A user who illegally obtains the identification or access details of another user is subject to a fine of up to JPY 1 million (approximately $9,199) or up to three years imprisonment.

Improper usage of those details, such as providing it to a third-party or impersonating the original user, may result in a JPY 500,000 fine (approximately $4,599) or up to a year imprisonment. The Penal Code provides more details on criminal sanctions and monetary penalties that can be issued for giving "improper commands", such as computer viruses. In addition, the Penal Code punishes those who obstruct another's business operations through improper computer access and usage with up to JPY 1 million (approximately $9,199) or up to five years imprisonment.[103]

The UCAL details multiple cybersecurity offences that many other countries are not as explicit about in their regulations. This includes hacking, denial-of-service attacks, phishing, malware, possession of hacking tools, identity theft/fraud, amongst others.[104]

Malaysia

Malaysia has a series of sporadic laws related to cybersecurity rather than a single, standalone law, though some agencies, such as CyberSecurity Malaysia, are working with the Ministry of Science, Technology and Innovation to suggest amendments and revamp cyber laws.[105] The range of existing laws in place to counter cybercrimes is quite extensive:[106]

1. Computer Crimes Act 1997 (CCA)
2. Communications and Multimedia Act 1998 (CMA)
3. Penal Code
4. Copyright Act 1987
5. Personal Data Protection Act 2010
6. Digital Signature Act 1997
7. Strategic Trade Act 2010
8. Sedition Act 1948
9. Case laws

Other specific guidelines/policies:

The CCA outlines penalties for hackers, including to a fine of up to RM 150,000 (approximately $36,000) and/or up to five years imprisonment. There are no specific offences regarding denial-of-service attacks or phishing, though some provisions in the CMA and Penal Code may cover this. Infecting a system with malware, however, is punishable under the CCA with RM 100,000 (approximately $24,000) or up to 10 years imprisonment.

The largest fines issued are for possession of hacking tools and for copyright infringement involving trade secrets and intellectual property - a person found guilty in either case is liable for a fine of up to RM 500,000 (approximately $120,200) and/or up to five and ten years imprisonment respectively.[107]

[103] Hayashi 2018
[104] Hayashi 2018
[105] CyberSecurity Malaysia n.d.
[106] Yik 2018
[107] Pillai and Han 2018

Singapore

Singapore's Cybersecurity Act was passed and came into force in 2018. The new law establishes a regulatory framework for oversight and maintenance of national cybersecurity in Singapore.

One of the four key objectives is to strengthen the protection of the nation's Critical Information Infrastructure (CII) against cyber-attacks. It imposes several obligations on the CII owners such as reporting cybersecurity incidents, undertaking audits of their CII every two years, and conducting annual risk assessments.

Another key objective is to establish a light-touch licensing framework for cybersecurity service providers, namely penetration testing and a managed security operations centre (SOC). This is due to their access to sensitive client information. If providers fail to obtain the necessary licence to provide cybersecurity services, they may be fined up to $50,000 or spend up to 2 years in prison.

Corporation employees who fail to comply with cybersecurity investigations may be fined up to $20,000 and/or imprisoned for up to 12 months. Additional penalties may be issued for failure to comply with specific items in the regulations and continuing offences.[108]

The remaining two objectives of the Act are to establish a framework for government, companies, and computer owners to share cybersecurity information, and to authorise the Commissioner of Cybersecurity to investigate threats and incidents in order to respond effectively.[109]

In addition to the 2018 Cybersecurity Act, the Maritime and Port Authority of Singapore launched a new cybersecurity operations centre in May 2019. Its focus is the early detection, 24/7 monitoring, and response to cybersecurity threats across all maritime CIIs.[110]

The Republic of Korea

Cybersecurity regulation in The Republic of Korea has no single overarching law, but rather a collection of statutes, provisions, guidelines, and regulations governing cybersecurity operations.[111]

1. The Act on the Promotion of IT Network Use and Information Protection (the Network Act)112
2. The Personal Information Protection Act (PIPA)
3. The Electronic Financial Transactions Act (EFTA)
4. The Regulation on Supervision of Electronic Financial Transactions (the RSEFT)
5. The Credit Information Use and Protection Act (the Credit Information Act)
6. The Act on the Protection and Use of Location Information (the Location Information Act)
7. The Protection of Information and Communications Infrastructure Act (PICIA)
8. The Act on Consumer Protection in Electronic Commerce
9. The Digital Signature Act
10. The Special Act on the Prevention of Loss Caused by Telecommunications-Based Financial Fraud and Refund for Loss (the Special Act on Financial Fraud)

Hacking is prohibited under the Network Act of 2009. A person found guilty of accessing a computer or system without permission of the owner will be fined KRW 50 million (approximately $42,400) or up to five years imprisonment. Under the EFTA, if the system accessed contains financial information or is a financial system, the offender is subject to a KRW 100 million fine (approximately $84,820) or up to 10 years imprisonment.

Denial-of-service attacks and phishing carry similar hefty penalties under the Network Act and the Special Act on Financial Fraud respectively. Distribution malware or possessing hacking tools are both prohibited under the Network Act and carry fines of up to KRW 70 million (approximately $59,370) or up to seven years imprisonment.[113]

[108] Singapore Statutes Online 2018
[109] Cyber Security Agency of Singapore 2019
[110] The Maritime Executive 2019
[111] Son and Kim 2019
[112] Government of the Republic of Korea 2009
[113] Choi and Jung 2018

China

The Cyber Security Law of the People's Republic of China (the China Internet Security Law) came into effect in June 2017 and has sparked much debate.[114] Cybersecurity experts are still unpacking all of the new provisions and regulations two years later.[115]

The law makes provisions to safeguard the sovereignty of cyberspace and the dissemination of socialist values, social morality, and national honour.[116]. In some areas, it seems to go beyond cybersecurity with the aim to regulate behaviour more generally, prohibiting the spreading of sexual information and fake news [117] as well regulating against attempts to circumvent the Great Firewall.[118]

Under this regulation, foreign companies may be required to provide source codes and encryption for review by authorities, raising concerns about data privacy and corporate espionage.[119] Corporations are required to store data on local servers governed by Chinese law.

In the wake of this announcement, Apple transferred operations of iCloud in Mainland China to a data company sponsored by the Chinese government, whereas online services like Skype and WhatsApp, which refused to store data locally, were banned from operating in the country or had their expansion plans restricted.[120]

Failure to comply with data localisation laws may result in a monetary penalty of up to RMB 500,000 (approximately $72,344). Network operators and personnel directly in charge may be subject to fines and imprisonment.[121]

[114] Wikipedia 2019
[115] Gritsi 2019
[116] Asia Briefing, Dezan Shira & Associates 2019
[117] Yahoo! Finance 2018
[118] Hill 2018
[119] Wagner 2017
[120] Wuerthele 2017
[121] Reed Smith 2018

Appendix C: Cyber vulnerabilities in the shipping industry

World trade depends on the reliability and health of the international shipping industry. Almost every aspect of the shipping industry lends itself to internet connectivity. Global positioning systems (GPS) allow ships to stay on course, reducing wait times; Marine Automatic Identification System (AIS) track and monitor ships, allowing suppliers and customers to know where their goods are and allow for 'just in time' timelines to develop for less spoiled goods and wasted warehouse time; Electronic Chart Display and Information Systems (ECDIS) and the associated digital nautical charts mean fewer crewmembers are needed, keeping costs down.

These are only a few of the technologies that have allowed the maritime industry to grow and continue supporting world trade. Worryingly, however, while the maritime industry has accepted the greater strides of cyber technologies to move them forward, it seems it has yet to fully acknowledge the potential for these same technologies to set them back with cyber-attacks.

Table 11: Age distribution of world merchant fleet by vessel type 2018[122]

	Average Years				
	0-4	5-9	10-14	15-19	20+
Oil tankers	15%	22%	17%	8%	38%
Dry bulk carriers	28%	41%	13%	9%	9%
General Cargo Ship	6%	16%	12%	7%	59%
Container Ships	2%	27%	27%	15%	14%
Other	13%	19%	12%	8%	47%
All Ships	14%	22%	13%	9%	42%

This table highlights the large percentages over 20 years of age.

Ships, like everything else, are now are part of a threat actor's cyber-attack surface.[123] They are one component in a long and time-sensitive supply chain. While it may seem that the maritime industry has been slow to acknowledge this, it is largely due to the combined complexities of the maritime industry and cyber security.

There are several different classes of maritime vessels, each with a designated design and purpose with different computer systems built to meet the requirements. Large container ships are expensive and take considerable time to build and are thus intended to be in use for at least thirty years. As seen in Table 11, nearly half of the ships that are currently on the seas are 20+ years old. Cyber technologies and security have made tremendous progress since then - nearly half of the ships on the seas right now could have been released before the internet was introduced in 1990. This changed the landscape for shipping security.

Because many of the ships on the sea today were built before cyber security was a major concern, their original infrastructure was not designed with updates in mind, leaving them to run unsupported operating systems and software. Furthermore, it is not uncommon for new software to be incompatible with older hardware, keeping outdated software systems in use out of necessity. Even in more modern ships, the systems of large vessels are often isolated at sea for extended periods of time, giving an attack plenty of time to spread through a system before it is addressed.[124]

An additional complexity is the crew. Ship crews are a dynamic aspect to the system of a ship, often changing quickly. As a result, crews are often using systems they are unfamiliar with, increasing the potential for both accidental and malicious cybersecurity incidents relating to human error. The complexities involved with onboard system maintenance often leads to outsourcing for IT support.[124]

[122] UNCTAD 2018

[123] Tam and Jones 2018

[124] Tam, Jones, and Papadaki 2016

Maintenance of cyber systems, including integral ones for navigation, are often contracted to third-party vendors, which means the crew are likely to be unfamiliar with the systems and may be ineffective in the event of a cyber-attack.

Communication is key in the shipping industry, which ties the systems onboard ships to their companions on land. The cybersecurity of the ship and land systems are thus interdependent with attacks on one providing an entryway to the other.

Areas of vulnerability

The shipping industry is investing heavily in technologies that have the potential to transform the maritime industry many aimed at reducing human error. Reports indicate that human error accounted for roughly 75% of the value of almost 15,000 marine liability insurance claims in 2011–2016, equivalent to over $1.6 billion.[125]

According to a 2019 maritime industry report, 90% of respondents believe their organizations will increase technology spending.[126] However, the new technologies onboard vessels are also vulnerable to failure, disruption, and interference.[127] The vulnerabilities can be broadly classified into system-related vulnerabilities, propagation-channel-related vulnerabilities, and interference-related vulnerabilities.

Electronic Chart Display and Information Systems (ECDIS): a geographic information system used for nautical navigation that complies with International Maritime Organization (IMO) regulations as an alternative to paper nautical charts.[128]

Global Navigational Satellite System (GNSS): Global Navigational Satellite Systems (GNSS) is a non-specific term for space-based systems, which transmit signals used for positioning, navigation, and timing. The most well-known GNSS is the Global Positioning System (GPS).[129]

Marine Automatic Identification System (AIS): Marine Automatic Identification Systems are used for tracking and monitoring ships by automatically exchanging information with surrounding parties. They are effective in monitoring traffic and avoiding vessel collisions and are useful for accident investigation and in search and rescue.[130]

Smart Ships: Ship operations are becoming increasingly computer controlled, which has allowed for greater efficiency in ship management. Referred to as Smart Ships, the vessels are built with increased automation in operational systems, system monitoring, and data communication, reducing the amount of human labour and allowing for faster and automatic industrial decisions with the aim that these ships will become autonomous.[131] It is still unclear whether these autonomous ships will be fully accepted by Governments and the maritime industry as a whole.[132]

[125] UNCTAD 2018
[126] Navis 2018
[127] Burnson 2015
[128] Bhattacharjee 2011; UKHO 2016
[129] "What Is GNSS?" 2016
[130] Bhattacharjee 2017; Marine Insight 2017
[131] Hellenic Shipping News Worldwide 2017; World Maritime News 2017
[132] UNCTAD 2018; CyberKeel 2014

Appendix D: Guide to insurance portfolio loss estimations

This guide provides the University of Cambridge Centre for Risk Studies' recommended guidelines for insurance companies to estimate losses from the 'Shen Cyber Attack on Ports' scenario.

Each subsection outlines the methodology and data required to estimate the insured loss for a particular cyber affirmative and non-affirmative coverage to aid in the estimation of an insurance portfolio.

This portfolio estimation method is adapted from the industry loss estimation and has been adjusted to provide a portfolio specific loss compared to the aggregated industry loss outlined in the report.

Identifying the claimants

Within this scenario, there are seven predominant claimant groups, each of which have a series of insurance policies which are claimed following the Shen Cyber Attack.

These claimant groups and their 2017 North American Industry Classification System (NAICS) number are summarised in Table 12, overleaf.

Table 12: Claimant type and 2017 NAICS number

Claimant	NAICS Number	NAICS Title	Corresponding index entries
Port Operators	488310	Port and Harbor Operations	– Port facility operation – Docking facility operation – Harbor operation – Waterfront terminal operation – Wharf operation
Perishable Cargo Content Owners			
Ship Owners			
Port Management System Software Providers	511210	Software Publishers	– Software publishers
	541614	Process, Physical Distribution, and Logistics Consulting Services	– Transportation management consulting services
Logistics and Cargo Handling Companies	488320	Marine Cargo Handling	– Loading and unloading services at ports and harbors – Longshoremen services – Marine cargo handling services – Stevedoring services
	488390	Other Support Activities for Water Transportation	– Cargo checkers, marine – Cargo surveyors, marine – Marine cargo checkers an surveyors
Ship Management Company	511210	Software Publishers	– Software publishers
	541330	Engineering Services	– Marine engineering services
	541614	Process, Physical Distribution, and Logistics Consulting Services	– Transportation management consulting services
	541690	Other Scientific and Technical Consulting Services	– Safety consulting services – Security consulting services
Supply Chain Companies			

The remainder of this section considers each of these claimants and describes the insurance lines and methodology specific to each party.

Port operators

Port Operators are defined as companies or boards who regulate and manage port and marine services, facilities, and activities within their associated jurisdictional waters. Within the scenario, we assume port operators claim on the following lines of insurance:

- Cyber
  - Business Interruption
- Commercial Property
  - Business Interruption
- Liability
  - Directors and Officers
- Cyber
  - Incident Response costs
  - Regulatory and Defense Coverage
  - Reputational Risk
  - Data and Software Loss

Many of the calculations are specific to the ports which are impacted by the virus. To pursue claimant loss modelling, you must first identify which port operators are affected by the virus.

Selecting the ports

This report describes three variants, which consider different ports across Asia, as summarised in Table 13. To select the port operators' policies impacted, group all your policies by their port location. Select your port exposure by port TEU turnover.[133] For example, select the top three ports by TEU turnover in Japan and then model losses for those port operators as follows. The selected ports will also be used to identify other losses.

Table 13: Scenario variant port selection

Scenario variant	Country	Number of impacted ports per country
S1	**Singapore**	1
S2	**Japan**	3
X1	**Malaysia**	2
	Korea	3
	China	6

The methodology for each insurance class is outlined below.

Business interruption

List the impacted ports. Assume that all the operations at the ports are suspended for a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure. The outage is consistent across all scenario variants.

Cyber affirmative

Select the port operators which are covered by a cyber affirmative policy and assume business interruption for a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure. Apply appropriate deductibles and limits for the business interruption, as per the policy terms for these accounts, and calculate the total business interruption loss for your portfolio.

Cyber non-affirmative, All Risks

Select the port operators which are covered by a cyber non-affirmative policy and assume business interruption for a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure. Apply appropriate deductibles and limits for the business interruption, as per the policy terms for these accounts, and calculate the total business interruption loss for your portfolio.

Liability: Directors and Officers

Cyber non-affirmative, All Risks

Of the port operators selected, identify how many have a D&O policy. For each policy, assume a loss of the maximum policy limit, as per the policy terms for these accounts.

[133] If you do not have the port's annual TEU turnover, refer to Lloyd's "One Hundred Ports" report, which lists the world's largest container ports. (Lloyd's 2018a)

Cyber: Incident Response Costs

Cyber affirmative

Of the port operators selected, identify those which have a Cyber Incident Response Policy. For each port covered by the policy, list the annual TEUs[134] and calculate an estimated daily rate.[135] Multiply the daily rate by $500 per day for incident response services to reach a loss estimate. See Equation 1. Apply appropriate limits and deductibles. If possible, apply sub-limits. Repeat this step for each port operator.

Equation 1: Cyber Reputational Risk Cost Methodology

$$Incident\ Response\ Costs = \ (Annual\ TEU\ turnover \div 365\ days) \times \$500\ per\ day$$

Cyber: Regulatory and Defense Coverage

Cyber affirmative

Of the port operators selected, identify how many have a Cyber Regulatory and Defense Policy. For each port, take the annual number of TEUs[136] and assume $1 loss per TEU. Assume an additional $10,000,000 worth of fines per port. See Equation 2. Apply appropriate limits and deductibles. If possible, apply sub-limits. Repeat this step for each port operator.

Equation 2: Cyber Reputational Risk Cost Methodology

$$Regualtory\ and\ Defense\ Coverage = \ (Annual\ TEU\ turnover \times \$1\ per\ TEU) + \$10{,}000{,}000$$

Cyber: Reputational Risk

Cyber affirmative

Of the port operators selected, identify how many have a Cyber Reputational Risk policy. For each policy, assume a loss of the maximum policy limit for the duration the ports are suspended (a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure). Repeat this step for each port operator.

Cyber: Data and Software Loss

Cyber affirmative

Of the port operators selected, identify how many have a Cyber Data and Software Loss Policy. For each policy, take the daily TEUs[137] and multiply it by the number of days the port is closed (a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure). Multiply the sum by $50 per TEU to determine the total cost. See Equation 3. Apply appropriate limits and deductibles. If possible, apply sub-limits. Repeat this step for each port operator.

Equation 3: Cyber data and software loss methodology

$$Cyber\ Data\ and\ Software\ Loss = \ (Annual\ TEU\ turnover \div 365\ days) \times\ of\ Days\ Port\ is\ Closed \times \$50\ per\ TEU$$

[134] If you do not have the port's annual TEU turnover, refer to Lloyd's "One Hundred Ports" report, which lists the world's largest container ports. (Lloyd's 2018a)

[135] When calculating the daily rate, take the annual TEU turnover, and divide the value by 365.

[136] If you do not have the port's annual TEU turnover, refer to Lloyd's "One Hundred Ports" report, which lists the world's largest container ports. (Lloyd's 2018a)

[137] When calculating the daily rate, take the annual TEU turnover (available at (Lloyd's 2018a)) and divide the value by 365.

Perishable cargo content owners

Perishable cargo content owners are either individuals or organizations that have paid for Perishable cargo under a legal contract. Perishable cargo is defined as "goods that will deteriorate over a given period of time or if exposed to adverse temperature, humidity or other environmental conditions".[138]Within the scenario, we assume perishable cargo content owners claim on:

- Marine
  - Cargo

The methodology used is summarised in the section below.

Marine: Cargo

Cyber affirmative

For each port identified above, identify how many insured TEUs pass through the port on an annual basis. Calculate the average daily rate by dividing the annual total by 365 days. If available, calculate what proportion of your marine cargo portfolio is perishable goods.[139] Apply the percentage of perishable goods to estimate the number of perishable TEUs per day.[140] Multiply by 75% to select the proportion of perishables which are damaged during the port suspension. Multiply the number of days the ports are suspended (closed (a period between 4 – 7 days which are the minimum and maximum outages in this report. Decide the duration based on your views about port capabilities and exposure). Multiply the sum by the average value of your insured perishable cargo.[141] See Equation 4.

Equation 4: Marine cargo loss methodology, perishable selection

$$\begin{aligned} &Perishable\ Cargo \\ &\quad = \big((Annual\ insured\ TEU\ turnover \div 365\ days) \\ &\quad \times Proportion\ of\ Portfolio\ which\ is\ Perishable\ (\%)\big) \times 75\% \times \#\ of\ Days\ Port\ is\ Closed \\ &\quad \times Average\ cost\ per\ TEU\ (\$) \end{aligned}$$

Apply the appropriate limits and deductibles. Exclude accounts that use CL380 wording, or that have territorial limits in their terms and conditions.

[138] ("Perishable Cargo Handling" 2019)

[139] If this figure is not available, assume 7% of your insured cargo is perishables.

[140] Within the scenario we assume that only perishable cargo claims for business interruption, all other cargo types will not be eligible for claims.

[141] If you do not know this value, assume the average value of a perishable TEU is $5,000

Ship-owners

Ship owners are the individuals or organizations responsible for the ownership and operation of the vessel. Within the scenario, we assume ship-owners claim on:

– Marine
  - Freight, Demurrage and Defense

The methodology used is summarised in the section below.

Marine: Freight, Demurrage and Defense

Cyber non-affirmative, All Risks

Assume that one ship per port faces extensive legal disputes due to the transmission of the virus. At each of your selected ports, identify one ship which operates out of the port, which is insured with Marine Freight, Demurrage and Defense coverage.[142] Select the ship with the highest policy limit. We assume the cost of legal fees is $15 million per ship. Apply appropriate limits, deductibles, and exclusions. Exclude accounts that use CL380 wording, or that have territorial limits in their terms and conditions. Sum the legal fees of all affected ships.

Port management system software providers

The Port Management System is a software application that supports the administration and operations of port operators in a range of tasks. Within the scenario, we assume Port Management System Software Providers claim on:

– Liability
  - Directors and Officers
  - Technology Errors and Omissions

Selecting the Port Management System

This scenario assumes that each port runs an independent port management system. If you know which port management system is used by the ports selected, continue this methodology using the known systems. If you do not know which port management system is used, identify which port management systems are insured in your cyber or marine portfolios, and rank by annual revenue. Select the port management systems with the highest revenue, assuming the same number of port management systems as number of ports, outlined in Table 13.[143]

The loss methodology is summarised in the sections below.

Liability: Directors and Officers

Cyber non-affirmative, All Risks

For each insured port management system, assume one $15 million D&O claim. Apply appropriate limits and deductibles. If possible, apply sub-limits. Repeat this step for each insured port management system.

Liability: Technology Errors and Omissions

Cyber non-affirmative, All Risks

For each insured port management system, assume one $10 million Tech E&O claim. Apply appropriate limits and deductibles. If possible, apply sub-limits. Calculate the total Tech E&O exposure for port management systems in your portfolio.

[142] If you do not have the port specific information, rank your Marine Freight, Demurrage and Defense policies by largest policy limit. Select the largest 6, 9, or 15 policies, depending on the scenario variant and number of infected ports, summarised in Table 13.

[143] If you do not insure as many port management systems at ports within this scenario, assume 60% of the port management systems within your portfolio make a claim.

Logistics and cargo handling companies

Logistics and Cargo Handling Companies provide key transportation support at ports. Within the scenario, Logistics and Cargo Handling Companies are infected from the port authority, and face data compromise and business interruption. Within the scenario, we assume they can claim on:

- Liability
  - Directors and Officers
- Cyber
  - Data and Software Loss
  - Business Interruption
- Commercial Property
  - Business Interruption

To select Logistics and Cargo Handling Companies, list all Logistics and Cargo Handling Companies which are insured in your portfolio, and rank based on annual revenue. Select in descending order the number of companies required for the scenario variant, summarised in Table 14.

Table 14: Logistics and cargo handling companies - scenario variant count

	S1	S2	X1
Number of logistics and cargo handling companies	24	36	60

The methodology used to estimate the insured loss is summarised in the section below.

Liability: Directors and Officers

Cyber non-affirmative, All Risks

Assume that each Logistics and Cargo Handling Company has one D&O claim of $7 million. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Cyber: Data and software loss

Cyber affirmative

Assume that each Logistics and Cargo Handling Company has one data and software claim of $25 million. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Business Interruption

Cyber affirmative

Of the chosen Logistics and Cargo Handling Companies, select those which are covered by a cyber affirmative policy and assume business interruption of 7 days. Apply appropriate deductibles and limits for the business interruption, as per the policy terms for these accounts, and calculate the total business interruption loss for your portfolio.

Cyber non-affirmative, All Risks

Of the chosen Logistics and Cargo Handling Companies, select those which are covered by a cyber non-affirmative policy and assume business interruption of 7 days. Apply appropriate deductibles and limits for the business interruption, as per the policy terms for these accounts, and calculate the total business interruption loss for your portfolio.

Ship management company

The Ship Management Company is a company independent of the owner of the ship which maintains and operates the vessel. Within the scenario, we assume one Ship Management Company is compromised and is responsible to introducing the virus to multiple ports. We assume the Ship Management Company claims on:

- Liability
  - Technology Errors and Omissions
  - Directors and Officers
- Cyber
  - Data and Software Loss

To select the Ship Management Company, list all ship management companies which are insured in your portfolio, and rank based on annual revenue. Select the ship management company with the highest revenue.

The methodology used to estimate the insured loss is summarised in the section below.

Liability: Technology Errors and Omissions

Cyber non-affirmative, All Risks

Assume that the Ship Management Company has one Tech E&O claim of $20 million. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Liability: Directors and Officers

Cyber non-affirmative, All Risks

Assume that the Ship Management Company has one D&O claim of $15 million. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Supply chain companies

Third-party organizations who are indirectly impacted considers those who are impacted further along the supply chain. Within the scenario, we assume Third-party organizations claim on:

- Commercial Property
  - Contingent Business Interruption
- Cyber
  - Contingent Business Interruption

Commercial property: Contingent business interruption

Cyber non-affirmative, All Risks

Identify accounts in your portfolio that have CBI on their property insurance policies or Cyber Non-Affirmative Contingent Business Interruption policy, with locations based on the distribution in Table 15.

Table 15: Distribution of indirect economic loss exposure

Region	S1	S2	X1
America	6%	6%	5%
Asia	79%	79%	80%
Europe	13%	13%	13%
Rest of World	2%	2%	2%

Exclude accounts that use CL380 wording, or that have territorial limits in their terms and conditions. Rank the selected accounts by size and select the top percentages of accounts as specified in Table 16 and assume that they have the specified total number of interrupted business days. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Table 16: Proportion of accounts and business interruption durations to be assumed for policies with Business Interruption cover

Scenario Variant		Top	Next	Final	Total % of Accounts
S1	**% of Accounts**	2%	8%	10%	20%
	Days of BI	*8*	*6*	*4*	
S2	**% of Accounts**	3%	12%	15%	30%
	Days of BI	*10*	*8*	*6*	
X1	**% of Accounts**	5%	15%	20%	40%
	Days of BI	*15*	*10*	*8*	

Cyber: Contingent business interruption

Cyber affirmative

Identify accounts in your portfolio that have a Cyber Affirmative Contingent Business Interruption policy, with locations based on the distribution in Table 15. Exclude accounts that use CL380 wording, or that have territorial limits in their terms and conditions. Rank the selected accounts by size and select the top percentages of accounts as specified in Table 16 and assume that they have the specified total number of interrupted business days. Apply appropriate limits and deductibles. If possible, apply sub-limits.

Total

Total all the components of loss into a grand total of losses for your portfolio.

CyRiM Report 2019

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
LLOYD'S
AON Empower Results®
MSIG
SCOR The Art & Science of Risk
TransRe We value risk.
Centre for Risk Studies
UNIVERSITY OF CAMBRIDGE Judge Business School