Maritime Supply Chain Security in the Indo-Pacific Region: Threats and Policy Implications for National Security and Resilience

To Ensure the Peace, Prosperity, and Sustainability of the Indo-Pacific Region

Hong-Oanh Nguyen, Michael Van Balen, Aaron Ingram, Stephen Hurd,
Prem Chhetri, Vinh Thai, Matthew Warren, Booi Kam,
Richard Oloruntoba

31 May, 2022

Acknowledgement

This report is an output of the Project Grant 202021-0239, Strategic Policy Grants Program 2021, funded by Australian Department of Defence.

The views expressed herein are those of the authors and are not necessarily those of the Australian Government, the Australian Department of Defence, University of Tasmania, RMIT University or Curtin University.

The project team would like to thank the participants attending the Indo-Pacific Maritime Supply Chain Security Focus Group Workshop for their contribution to the success of the workshop.

Throughout the project's implementation period, a number of people have made contribution and provide assistance to the project team. Maneerat Kanrak provided assistance in the collection and processing of shipping network data and Endnote preparation. Judy Crees-Morris provided support in preparation and organisation of the Focus Group Workshop and Stakeholder Workshop, proofreading and project administration. Carol Harding was the facilitator of the Focus Group and Stakeholder Workshops. Susan Oommen provided assistance in literature search.

Contents

Executive summary

By volume, about 99% of Australia's trade is carried by sea mainly through the Indo-Pacific region. Australia currently imports 90% of liquid fuel from other countries, primarily Japan, Korea and Singapore. Global shipping trade valued around USD3.37 trillion is also passed through the South China Sea, where Strait of Malacca is one of the busiest oil/energy shipping routes in the world. The region especially the South China Sea and East China Sea is subject to increasing maritime security threats due to territorial disputes and the risk of military conflicts. This report presents emerging security challenges facing maritime supply chains in the Indo-Pacific region and the implications for Australia. The report comprises four component studies.

The first study is a scenario analysis of maritime security threats in the South China Sea and the broader Indo-Pacific that are associated with three contexts, South China Sea conflict, cyber attack on Australian maritime information systems, and Indo-Pacific maritime logistics network disruption. The result of the scenario analysis indicates that South China Sea conflicts would cause shipping capacity shortage, port operations breakdown, production disruption, technology failures, international armed conflicts, trade sanctions/embargo and diversion. These will likely result in an economic downturn, critical supplies, maritime supply chain disruptions, and increasing military activities in the region.

Cyber attacks on Australian maritime information systems will cause navigation operations disruption, cyber operations disruption, social technical disruption, human resource issues (due to temporary skill shortages), and maritime supply chain disruption. These in turn have further impacts on Australia including port congestion and disruption of commercial shipping and supply chain operations.

Disruption of the Indo-Pacific maritime logistics network can caused by factors other than those mentioned above. These can be competitive responses/interaction between countries or large organisations; disruptive innovation, e.g. Northern Sea Route, and Belt and Road Initiative; geopolitical disruptions; ecological disruptions, e.g. tsunamis, pandemic, climate change; and trade related disruptions. These could have impacts on Australia including disruption of IT systems and trade networks, port and shipping operations, supply chain operations, critical supply shortages, loss of human lives, exhaustion of emergency rescue and security capabilities, economic downturn and social unrest.

The second study analyses the vulnerability of the tanker shipping network that Australia relies on for fuel supplies using Auto Identification System data. The analysis result indicates that while Australia's energy trade with Malaysia, Indonesia, Singapore, the US, Japan, Taiwan (China), Vietnam and the Philippines is not critically exposed to maritime security threats in South China Sea and East China Sea, energy trade of the latter countries is substantially exposed to tanker operations disruption caused by a closure of the South China Sea and East China Sea. All shipping routes connected to Taiwan will be directly impacted and so will all imports to Brunei. Seven out of eight shipping routes to Japan are affected and six of them are subject to a very significant impact. Six out of ten shipping routes to Malaysia, four out of fourteen routes to Singapore, and two out of seven routes to Thailand will be affected. The closure of the South China Sea and East China Sea will force tankers to avoid these seas causing tanker tonnage shortages and disruption of the fuel supply chains. As a result, Australia may join allies and other countries in the region in ensuring the Freedom of Navigation Operations (FONOPS) and upholding the rules-based international maritime order.

The third study highlights the vulnerabilities of the Australian maritime industry due to cyber-attacks and analyses the potential impact of cyber attacks on Australian maritime information systems under five cyber security threat scenarios, namely attacks on Australian destined shipping in the Malacca Straits; attacks on Australian bound shipping in the Lombok Strait; attacks on Australian bound

shipping due to ransomware cyber breaches; maritime supply chain disruption due to data breach; maritime supply chain disruption due to cyber blockade.

The third study also provides a number of recommendations for cyber security, including back-up system development, ransomware policy; adopting international cybersecurity standards and guidelines; improving the security of corporate information systems; strengthening the incident reporting systems; improving the security of electronic navigation systems; diversifying supply sources; formulating strategic alliances and partnership with countries; onshoring and nearshoring to avoid the conflict areas; building cyber resilience; incorporating cyber security in maritime training and education; and the Government's initiatives on maritime cyber security.

The fourth study proposes a national security-resilience framework for maritime supply chains, recapitulates security threats and advances strategies to enhance preparation and prevention, recovery from and adaptation to supply chain disruptions in the Indo-Pacific region. A focus group workshop was held to identify national security risks; resource and capacity constraints; and draw policy implications and recommendations for national resilience strategies.

Several security issues and constraints facing Australia's maritime supply chains identified include: reliance on one or few countries for critical supplies and main trade; the lack of ownership and control of a strategic fleet; insufficient stockpiles and fuel reserves; risk of disconnected to allies and partners in the Indo-Pacific in case of maritime territorial conflict; political influences on the Indo-Pacific region affecting Australia's strategic position; insufficient maritime infrastructure and the management of foreign investment in critical maritime infrastructure; natural disaster and climate change effects.

The strategic policy recommendations to address the above security risks and constraints include: increasing of stockpiles and critical reserves and the diversification of supply sources and supply chains to mitigate the risk of reliance on a few sources for critical supplies; development of reliable domestic production capacity; better control and development of a strategic fleet and maritime infrastructure; the Government taking the leading role in national resilience through active engagement with the private sector, public-private partnership and the participatory approach; the Government leading national preparedness and resilience building by promoting national awareness and consciousness of the security and resilience issues. Australia should take a more active role in the region through international relations and cooperation, focusing not only on the warfare and defence elements but also shifting trade patterns and building alliances with friendly countries in the region.

List of figures

List of tables

List of abbreviations

AIS	Automatic identification system
ANZUS	Australia, New Zealand and US
AUKUS	Trilateral security pact between Australia, the UK and the US
DDoS	Distributed denial-of-service
ECDIS	Electronic chart display and information system
ECS	East China Sea
FONOPS	Freedom of navigation operations
GLONASS	Russian global satellite system
GMDSS	Global maritime distress and safety system
GNSS	Global navigation satellite system
GPS	Global Positioning System
IEA	International energy agency
IMO	International maritime organisation
IPR	Indo-Pacific region
LPG	Liquefied Petrol Gas
LNG	Liquefied Natural Gas
NAVTEX	Navigation telex
QUAD	Quadrilateral security dialogue
RATs	Rapid Antigen Tests
SCS	South China Sea
SLOC	Sea lines of communication
UNCLOS	United Nations Convention on the Law of the Sea
WTO	World Trade Organisation

1. INTRODUCTION

National security is the security of a country, including its citizens, economy, and institutions. (https://en.wikipedia.org/wiki/National_security). Security can be broadly defined as "the preservation of the norms, rules, institutions and values of society" (Makinda, 1998). Security threats can be both military and non-military. Examples of the latter are pandemics, natural disasters, and cyber-attacks. Regarding the former, Senator Linda Reynolds, former Minister for Defence (2019), noted that:

> "the character of warfare is changing, with more options for pursuing strategic ends just below the threshold of traditional armed conflict – what some experts like to call grey-zone tactics or hybrid warfare."

About 99% of Australia's trade by volume is carried by sea mainly through the Indo-Pacific region (IPR) with two thirds of exports passing through the South China Sea (SCS) (Royal Australian Navy, 2017). Fuel supply is critical to the Australian economy. Yet, the country currently imports 90% of its liquid fuel and does not have sufficient to meet the 90-day stockholding requirement of the International Energy Agency (IEA). This indicates that Australia is vulnerable and would be fuel-insecure if there was a fuel supply chain disruption.

The IPR comprises the waters of the Indian Ocean, the western and central Pacific Ocean, and the seas connecting the two in the general area of Indonesia (Figure 1.1). The label 'Indo-Pacific' has recently replaced the 'Asia-Pacific' as a terminology for a broader region, as shown in Figure 1.1 (Medcalf, 2018, Yoshihara, 2013).While there are variations in definitions, a more practical understanding of the IPR can be gained through an appreciation of the interconnectedness and the interdependence of the two oceanic regions. This is a result of globalisation, trade and interaction between various actors that has broken down older boundaries and opened up new avenues in the last sixty or so years (Das, 2019). The IPR has become the global centre of economic development and is largely driven by commercial maritime activity and the assurance of its security by the US and to a lesser extent by the emergence of Japan and Australia as vital regional partners in maintaining security (Buszynski, 2012, Gopal, 2017).

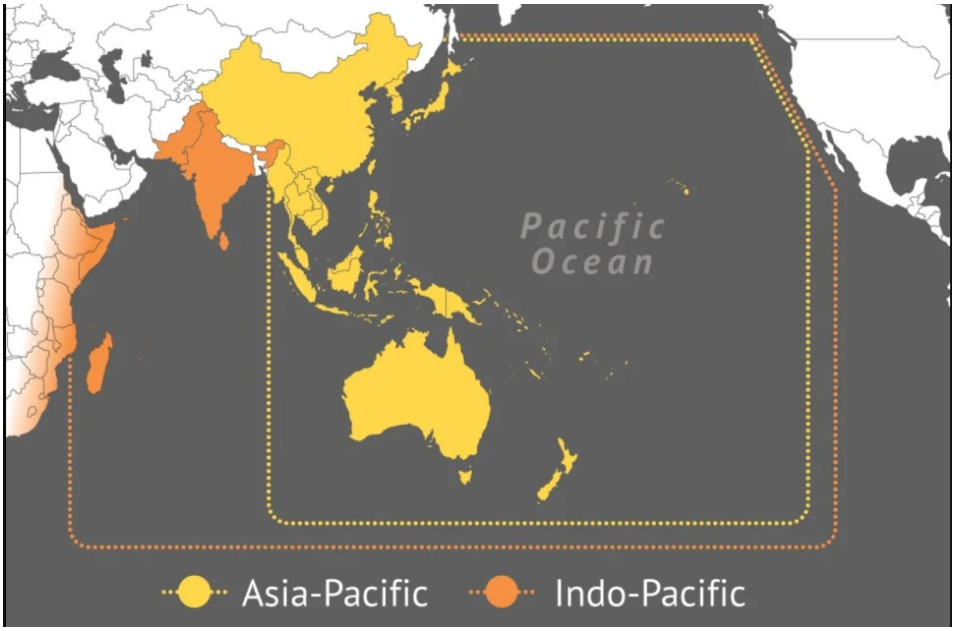


Figure 1.1: Indo-Pacific region (Galloway, 2021)

The rise of China and India politically and economically is changing the strategic balance between traditional global actors such as the US and the UK (Satake and Sahashi, 2021) and these newly emerging economies. Other than globalisation, several key developments have attracted attention to the IPR, these being (1) the growing political, economic, and military footprint of China in the IPR, (2) the relative decline of the US and its allies in the region (Asian et al., 2020), and (3) the strategic role of the IPR in global supply chains and markets with the two most populous nations. Figure 1.2 shows the shipping activity in the IPR.

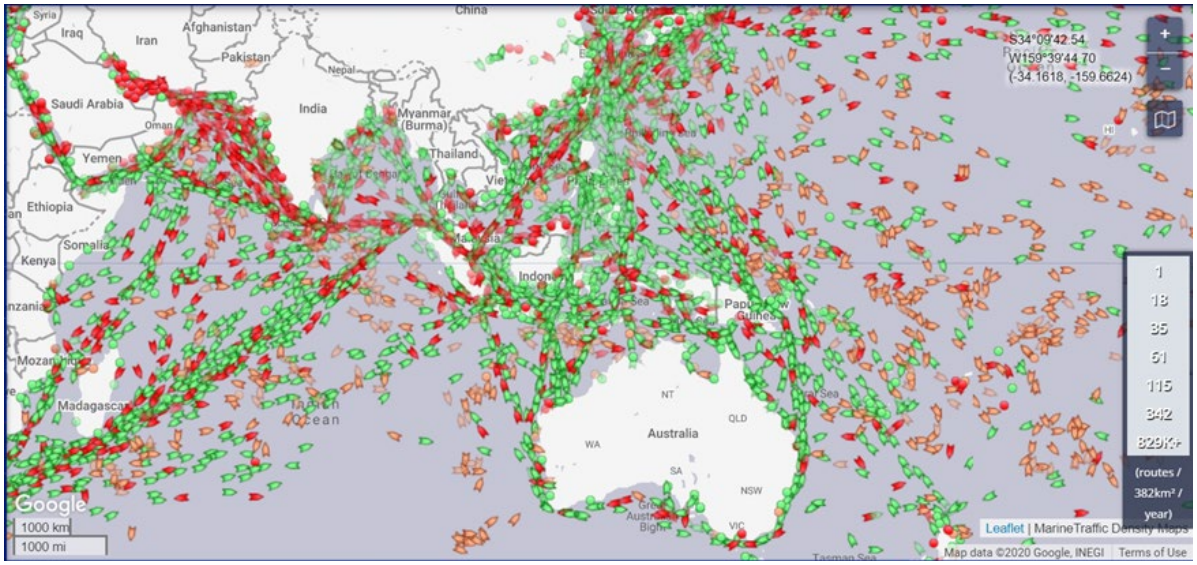


Figure 1.2: Shipping activity in Indo-Pacific region

China's political, economic and military rise has been manifested in (1) its maritime territorial claims and the 'seizing' of a string of strategic islands in the Indian Ocean (Yoshihara, 2013), (2) the *Belt and Road Initiative* in trade connectivity and maritime infrastructure; modernisation and growth of China's military capabilities (The Guardian, 2021), (3) the decline in economic and political influence of the U.S and its allies in the IPR (Oliveira, 2021), (4) contestation by other littoral countries such as Australia, Japan, Philippines, Vietnam, and Indonesia with complex maritime disputes, (5) the effort to counterbalance China's increasing geo-presence; the increasing geo-economic significance of China in the IPR, and (6) the restructuring of supply chains to reduce reliance on China (He and Li, 2020, Li, 2019).

Allocated in the centre of the IPR is the SCS where global shipping trade of around USD3.37 trillion passed through in 2016 (Villar and Hamilton, 2017). The Strait of Malacca serves as the doorway to the SCS and is the second-busiest oil/energy shipping route after the Straits of Hormuz. Sunda Strait and Lombok Strait are also important to Australia's maritime link to Asian countries (see Figure 1.3).

The SCS has been subject to increasing maritime territorial disputes and attempts to militarise disputed islands (Center for Preventive Action, 2022, Zahir, 2021). China's increasing assertiveness and coercion on its territorial claims in the SCS based on the U-shaped nine dash line (Beech, 2016, Dolven et al., 2021) have been a cause for security concern in the region and directly challenge US strategic primacy to ensure Freedom of Navigation Operations (FONOPS) and uphold "the rules-based international maritime order" (Davis, 2019, Price, 2021, Zahir, 2021). The SCS could thus become a flashpoint of military conflicts[1] (Rosales, 2019, Zhao, 2020) given the traditional threats e.g. piracy, maritime accidents, armed robbery, and non-traditional threats e.g. the use of grey zone tactics, land

[1] Some scholars e.g. Taylor (2014) argued that South China Sea is not a flashpoint.

reclamation and instalment of military equipment on land reclaimed from the sea, economic and trade coercion and cyber-attacks against shipping and ports (Beech, 2016, Tillett and Connors, 2020).

Figure 1.3: Chokepoints in the South China Sea (Villar and Hamilton, 2017)

Overall, the crucial importance of Australia's maritime supply chains and seaborne trade may be buttressed by the fact that Australia is the 5th largest user of shipping services in the world. Over 99% Australia's trade by volume and 79% by value is transported by sea. In the 2017-19 period, the combined value of Australia's seagoing international imports and exports was over $600 billion. Over 5,879 ships made a total of 32,801 port calls at Australian ports in 2016-17 including 5,743 cargo ships which made 17,068 voyages to Australian waters from overseas ports. In 2016, 10 Australian ports accounted for 88% of seaborne export cargo (Australian Naval Institute and Naval Studies Group, 2020).

About two thirds of Australia's exports pass through the SCS (Department of Defence, 2016, Department of Defence, 2020). Almost 100% of Australia's energy and commodity imports are transported through the choke points in SCS (Figure 1.3). Therefore, FONOPS is critical to Australia, especially in the areas of energy security and international trade.

While Australia is a close ally of the US, the Australian economy has been significantly dependent on China (Yilmaz and Liu, 2022). However, the unequal trade between China and Australia puts Australia in an economically vulnerable position. It is unduly reliant on the single market, putting the country at risk of market vitality, protectionism, and trade weaponisation (Di Lieto, 2018) (Jain, 2021).

The onset of COVID-19 and its impact on logistics and transport, including the export restrictions on various essential goods by some countries, has raised concerns about Australia's ability to sustain critical supplies. According to the Productivity Commission (2021), 5950 different products were imported in 2016-17 with a combined value of A$272 billion, equivalent to around 16% of the gross national income. However, the majority of imports is sourced from only five countries, China, the US, Japan, Thailand and Germany. There has been a shift in Australia's international trade towards the export of raw minerals and unprocessed agricultural products and import of manufactured, critical and essential products e.g. motor vehicles and parts, fuel, pharmaceuticals, biopharmaceuticals/

medicines, and agro-chemicals. This increases the vulnerability of the country to supply chain disruption and foreign influences.

Maritime security threats in the IPR can severely affect Australian economy and trade. The country needs evidence-based strategies and policies to keep its critical sea routes free from disruptions:

> "*Australia can never take its maritime trade for granted and the effects of disruption should never be underestimated. Ensuring freedom of navigation and the integrity and stability of sea lines of communication (SLOC) therefore remain important functions of naval forces*" (RAN, 2017). Moreover, "*we have a deep stake in the security of Southeast Asia, as any hostile forces would have to operate in this area to sustainably project force against us*" (Royal Australian Navy, 2010).

To protect national security, Australia relies on close allies through the Australia, New Zealand and US (ANZUS) Security Treaty), the Quadrilateral Security Dialogue (QUAD), and the trilateral security pact between Australia, the UK and the US (AUKUS). To reduce economic and supply chain vulnerability to China's economic coercion and counter China's supply chain dominance in the IPR and SCS, the governments of Australia, India and Japan launched a trilateral agreement, the Supply Chain Resilience Initiative, on 28 April 2021 (Department of Foreign Affairs and Trade, 2022). Australia, India and Indonesia have also formed a new trilateral bloc (Tillett and Connors, 2020). These initiatives aim to diversify the supply chains, strengthen supply chain resilience in the IPR and achieve long-term strong, balanced and inclusive growth of these countries.

This report presents emerging security challenges facing maritime supply chains in the Indo-Pacific region and the implications for Australia. The Section 2 identifies the key Indo-Pacific maritime supply chain security challenges facing Australia. Sections 3 and 4 present an analysis of the vulnerability of Australian maritime supply chains that are exposed to maritime transport and cyber security issues in the IPR. Section 5 presents a policy analysis and discusses strategic implications for Australia.

2. MARITIME SECURITY THREAT SCENARIOS IN THE SOUTH CHINA SEA AND THE INDO-PACIFIC REGION

2.1. Scenario development

Directed at issues sensitive to stakeholders, scenario development provides a means for decision-makers to anticipate forthcoming changes to mitigate likely impacts. Each scenario considers how the future might eventuate by analysing the past and current situation and creating informed assumptions (Mahmoud et al., 2009). In this study, scenario development was used to build plausible maritime security threat scenarios in the South China Sea and the broader Indo-Pacific region. The process entailed identifying past and current environmental pointers and constructing expressive images based on possible, and plausible, future happenings in the region, and was undertaken in the context of Australian national security from a maritime supply chain perspective.

The scenarios were first developed based on a desk review of relevant international research (e.g., published diplomat documents, military analysts' reports), and then deliberated through a scenario thinking workshop informed by reconstructed historical accounts, media commentaries and geopolitical debates. The scenarios with the most significant uncertainties were selected for further consideration, the identification of possible outcomes and the development of policy recommendations. Three contexts were identified for the scenario thinking exercise: (1) conflict in the SCS (Figure 2.1), (2) cyber-attacks on Australian maritime related IT systems, and (3) Indo-Pacific maritime logistics network disruption.

Figure 2.1: Disputed area in the South China Sea (BBC, 2020)

2.2. Scenario thinking method

Scenario thinking is a group thinking process, which facilitates knowledge sharing and strategic conversations to create stories about possible futures. This process was applied as the primary methodology for this study to enhance a deeper and collective understanding of what the future of maritime security might look like. A deliberative participatory process was adopted where all viewpoints were considered equal, and all ideas were discussed.

A scenario thinking internal workshop was organised to develop maritime security threat scenarios in the SCS and the broader IPR. The scenario narratives developed from the workshop were used for the maritime and cyber security impact analysis and policy analysis and recommendations.

A five-stage scenario thinking process was conducted in which participants first explored key disruptions under three different situational contexts, identified latent clusters and then created scenario narratives for impact analysis and discussion of implications. The scenarios were based on a five-to-ten-year planning horizon.

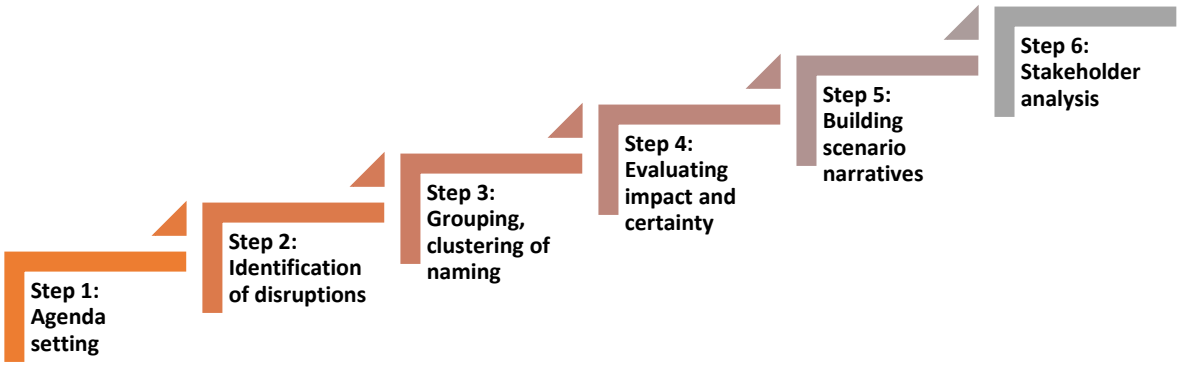


Figure 2.2: Scenario thinking process

In Step 2, the process of key disruptions/threats identification/listing was conducted first on an individual basis, so that each participant identified as many disruptions as they could think of in the allocated time. These disruptions/threats were recorded individually, each on separate e-Post-it® note (via Microsoft Whiteboard) without any discussion within the group.

Clustering of these threats was Step 3 of the Scenario Thinking process, which identified a smaller number of higher-order dimension(s) from the disruptions. The identified disruptions/threats were clustered, ensuring coherence within each cluster, through a group process of action discussion and consensus building. Step 4 was the development of plausible scenarios using the two key disruption dimensions, namely impact and certainty (likelihood).

In Step 5, the scoping of the future outcomes for the security threats to the maritime supply chain infrastructure and trade was conducted through an in-depth discussion of the two dimensions aimed at answering “what if?”. Answering this question aids in the development of scenario narratives.

The stakeholder analysis, in Step 6, identified the actors, e.g. government departments, international institutions, industry associations and businesses which have varying levels of power to and interest in shaping and/or managing scenario impacts. Interest represents the level of concern by the stakeholder, while power represents the level of authority to influence or implement change. Power is also the capacity to influence behaviour, cause change or ability to restructure situations. A matrix with two axes, namely power and interest, was generated to identify key stakeholders directly

involved in the planning and management of maritime supply chain security threats in the IPR. An analysis based on the power and interest of key stakeholders able to shape the plausible changes was also carried out. The following sections 2.3-2.5 present the three contexts covered in the scenario thinking exercise, namely, (1) SCS conflict, (2) cyber-attack on Australian maritime related IT systems, and (3) Indo-Pacific maritime logistics network disruption.

2.3. Context 1: South China Sea conflict

2.3.1. Key disruptions

The focus of this context is fuel supply chain disruption, on the backdrop of SCS conflict. The participants were asked: "What are the potential major disruptions to the Australian fuel maritime supply chain?" A total of 35 potential major supply disruptions were identified from the discussion and then grouped into the following six 'higher order dimensions':

i. Shipping Capacity Reduction
ii. Port Operations Breakdown
iii. Production Disruption
iv. Technology Failures
v. International Armed Conflicts
vi. Trade Sanctions/Embargo and Diversion

Shipping Capacity Reduction is caused by oil tankers diverted or re-routed to avoid dangerous areas, accidents, harassment of shipping.

Port Operations Breakdown stems from port closure, port congestion and associated delays.

Production Disruptions are caused by supply chain disruption, unexpected shutdown, depletion of fuel reserve, and shortage of fuel supplies caused by shipping capacity reduction.

Technology Failures refer to those of autonomous submersible vehicles, port supply network disruption, including rail and road as well as satellite services denial.

International Armed Conflicts can be but are not limited to military conflicts, threats from state or non-state actors and armed robbery.

Trade Sanctions/Embargos and Diversion refer to those caused by trade war and embargos with cascading effects on for examples aviation disruption, boom in grey oil markets, power network disruptions, and other disruptions to downstream industries, such as agricultural, fertiliser, pharmaceuticals, paints and solvents, plastics.

2.3.2. Impact and certainty

The next stage in scenario thinking is the generation of an impact and certainty matrix. This matrix reveals the impact and certainty/likelihood of each possible outcome of the studied event. As shown in Figure 2.3, Shipping Capacity Reduction is in the low-impact high-certainty quadrant indicating this outcome is low impact but is likely. Port Operation Breakdown, Production Disruption and Technology Failure are in the high-impact high-certainty quadrant. International Armed Conflict and Trade Sanctions/Embargo and Diversion have high impact but low certainty.

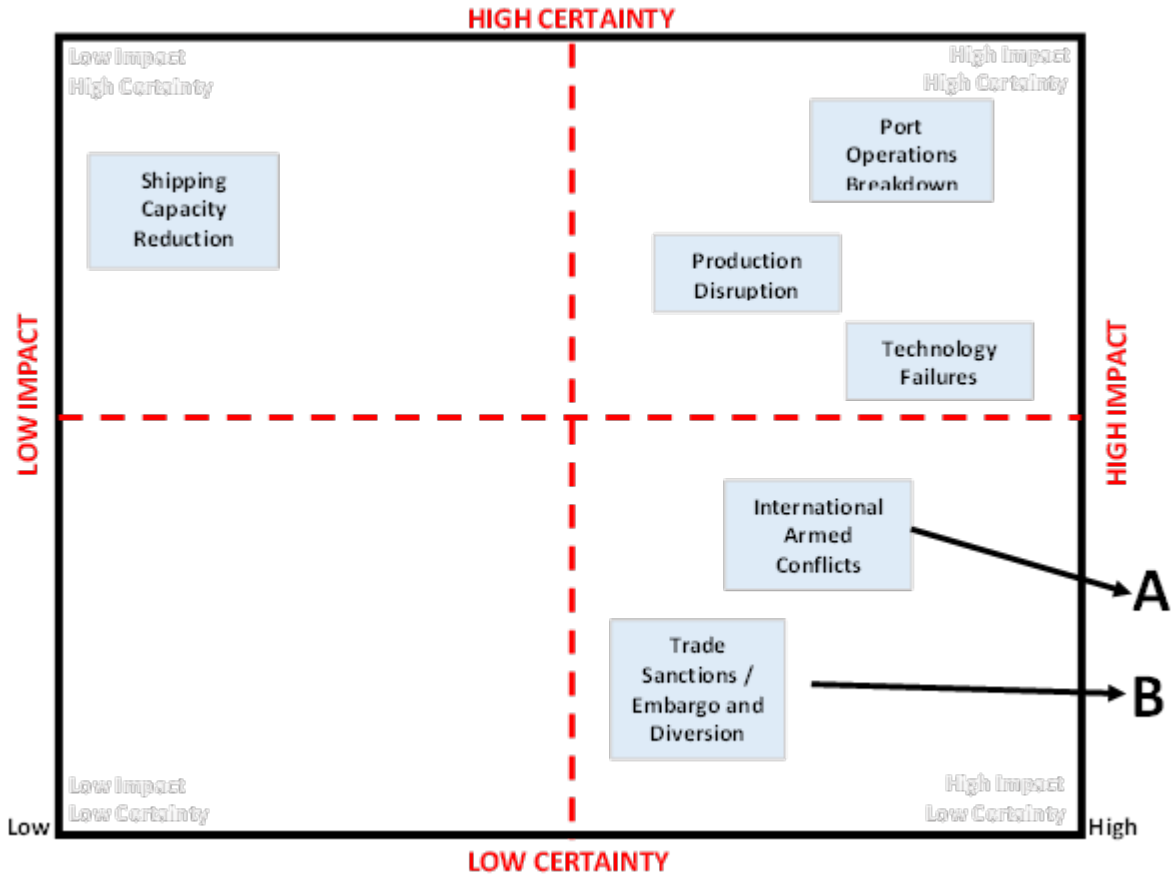


Figure 2.3: Certainty and impact of SCS conflict on fuel supply chain security

2.3.3. Framing and scoping the scenarios

Scoping of the future outcomes for fuel supply chain disruption was conducted through an in-depth discussion between participants on the two key effects, namely International Armed Conflict and Trade Sanctions/Embargo and Diversion as shown Figure 2.4.

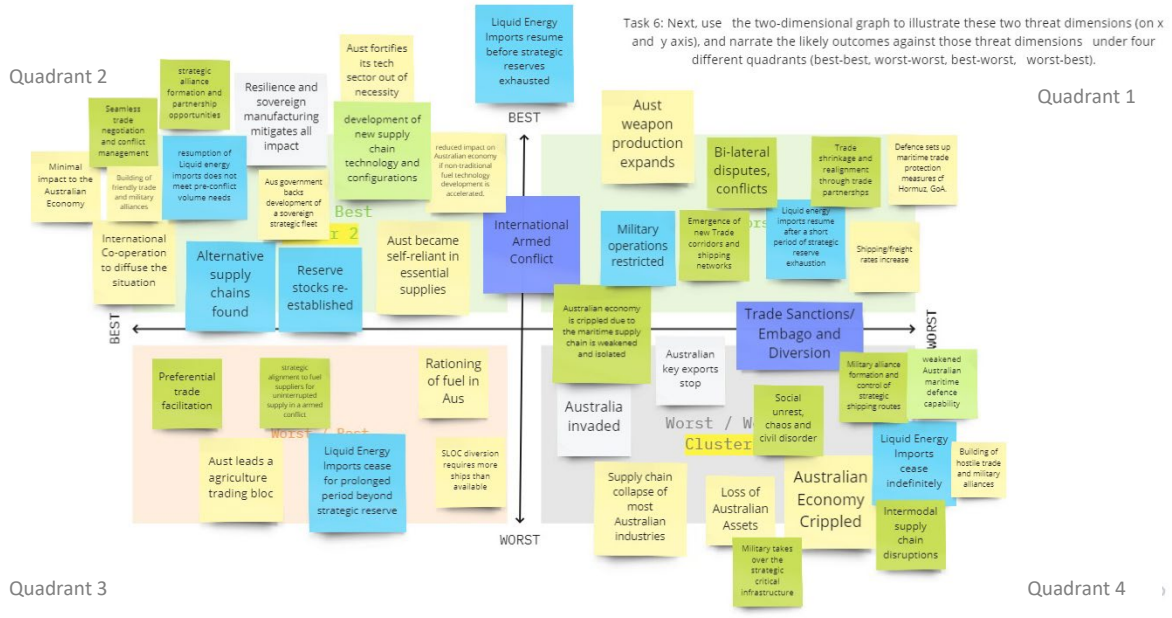


Figure 2.4: Plausible outcomes for Australia under different fuel supply chain scenarios

Participants were asked to consider the future impact of fuel supply breakdown on maritime supply chain and trade over the 10-year period. With the projected future impact and certainty of the dimensions in mind, participants discussed the broad possible and plausible scenario outcomes. 'International Armed Conflict' dimension is characterised by disruptions such as 'open conflict', 'grey zone war', 'attacks on vessels', 'sea mining', 'armed robbery', 'piracy', and 'laying of sea minefields in disputed waters'. Fuel supply disruptions in the Indo-Pacific region are more likely to be created by hostility and International Armed Conflict.

The Trade sanctions/Embargo/Diversion dimension covers various government actions and decisions on international trade. International sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organisations against states or organisations either to protect national security interests, or to protect international law, and defend against threats to international peace. A trade embargo is a governmental order to restrict trade of certain goods or all goods entirely with a foreign country. In some cases, embargoes lead to trade diversion where trade is diverted by transition through a third country to avoid the embargo resulting in higher prices of imported goods and economic inefficiency.

International Armed Conflict on the vertical axis and Trade Sanctions/Embargo and Diversion on the horizontal axis define the anchors for formulating the future scenarios. A consideration of the positive and negative aspects of the issues is the focus of the scoping and building of the scenarios. The dimensions were dissected into four quadrants to provide the basis for scenario building on a best-worst continuum. These quadrants represent a set of conditions to define four possible combinations. In other words, they describe best-best, best-worst, worst-best and worst-worst conditions in which the future of fuel supply chain disruptions might unfold. The quadrants represent a set of four well-defined possible maritime supply chain security outcomes. The best-best outcomes describe an 'ideal world', in which the scenarios described by the dimensions favour Australia's maritime supply chain.

The matrix represented in Quadrant 1 is the best of International Armed Conflict and worst of Trade Sanctions/Embargo and Diversion. Quadrant 2 represents the best of both International Armed Conflict and Trade Sanctions/Embargo and Diversion, while Quadrant 3 represents best of Trade Sanctions/Embargo and Diversion and worst of International Armed Conflict. Quadrant 4 represents worst of both International Armed Conflict and Trade Sanctions/Embargo and Diversion. The four scenarios formulated in the framework are not a prediction of the future, rather, an indication of the range of possible and plausible future outcomes under certain well-conceived conditions (Figure 2.4).

Worst-Worst Scenario: In quadrant 4, both International Armed Conflict and Trade Sanctions/Embargo and Diversion are at their worst. Australia may form military alliances, protect strategic shipping routes and take over the strategic critical infrastructure by military intervention. Other plausible outcomes of worst-worst scenario will be intermodal supply chain disruptions, resulting in the collapse of supply chains of most Australian industries and finally loss of Australian assets. This may eventually lead to crippling of the Australian economy, social unrest, and civil disorder and chaos. In a worst case of declared war/military conflicts in South China Sea, Australia may be invaded.

Best-Best Scenario: When both International Armed Conflict and Trade Sanctions/Embargo and Diversion are at their best, there will be minimal impact of the disruption to the Australian economy. In quadrant 2 seamless trade negotiation and conflict management will be achieved, and Australia will be able to protect its technology sector out of necessity with strategic alliance formation and partnership opportunities. Thus, the Australian government may enable development of a sovereign strategic fleet. In this scenario all outcomes are positive. The minimum impact of the disruption on

the Australian economy can be achieved if non-traditional fuel technology development is accelerated, reserve stocks re-established, and resilience and sovereign manufacturing mitigates all impact.

Best-Worst Scenario: Quadrant 1 represents best of International Armed Conflict and the worst of Trade Sanctions/Embargo and Diversion. Under this scenario, Australian military munitions production expands because of bi-lateral disputes and restriction in military operations, while conflicts shipping/freight rates increase, and liquid energy Imports cease indefinitely. The workshop concluded that at this scenario, there will be an emergence of New Trade corridors and shipping networks.

Worst-Best Scenario: In quadrant 3, is at its worst, while Trade Sanctions/Embargo and Diversion are at its best. Under this scenario, liquid energy imports may cease to exhaust all strategic fuel reserve in Australia, possible rationing of fuel for the general populace, which may force Australia to forge strategic alignment with fuel suppliers to support uninterrupted fuel supply in an armed conflict. Australia may need SLOC diversion to protect primary maritime routes between ports to support trade, transport and naval logistics as well as to sign preferential agreement to facilitate bilateral trade with strategic partners while taking up leadership of an agriculture trading block to sustain safe and efficient flow of commodities.

2.3.4. Plausible future outcomes

i. Maritime supply chains for exports and imports will be disrupted.

ii. Supply of critical goods such as fuel will decline.

iii. Australia may form military alliances to control strategic trade routes.

iv. Australia will build military alliances.

v. Australian economy will be affected.

2.4. Context 2: Cyber attack on Australian maritime information systems

2.4.1. Key disruptions

Context 2 focuses on exploring potential disruptions in the event of cyber-attacks and threats in the IPR. This is probed through the question: 'What are the major disruptions to the Australian maritime supply chain infrastructure and trade patterns within the Indo-Pacific Region in the context of a cyber-attack upon maritime IT systems?' Key disruptions were identified, discussed then grouped into the following dimensions:

i. Navigation Disruption and Maritime Security/Safety

ii. Cyber Physical Infrastructure Disruption

iii. Social Technical Disruption

iv. Human Issues

v. Maritime Supply Chain Disruption

Navigation Disruption and Maritime Security/Safety relates to: 1) hacking of systems that optimise and control processes at container ports and terminals affecting resilience of supply chains, 2) ransomware attacks (from both state threat actors and non-state threat actors) of systems, leading to loss of control of ships and their commodities, 3) disruption of ship and port navigation systems, and 4) illegally operating vessels in Exclusive Economic Zones due to port radar blindness. Issues like ransom, political demands, and terrorism compromise safe navigation and increase likelihood of major

maritime accidents. There is a risk of compromising freedom-of-navigations operations (FONOPS) due to navigation error, and potentially military conflict due to misunderstanding. Participants also warned the possibility of vessels becoming weapons due to an unauthorised party taking over the remote control of a vessel.

Cyber Physical Infrastructure Disruption include cyber attacks on ship-based systems, paralysis of port gates and truck loading as well as total disruption of port operations. Other issues and threats identified include infrastructure bottleneck, congestion, and delays with associated long queues at anchorages, cyber physical infrastructure disruption, ship route disruption and blockade, breakdown in ship/port automated system, disruption to terminal operations/cause major spill, vessels unable to berth, load or discharge and Australian maritime infrastructures completely disabled.

Socio Technical Disruption in maritime supply chains and trade patterns are driven by the interaction between complex societal infrastructures and organisational behaviour. This dimension is associated with issues, such as social unrest due to late arrival and shortage of commodities, protection of Australian aerospace IT infrastructure and re-creation of a new maritime digital ecosystem. All these impact Australia's critical infrastructures.

Human Resource Issues are behavioural in nature and are linked to accidents, re-emergence of former (pre-technical) seafaring skills, lack of human resources to replace automation systems to overcome the shortage of cyber security skills within Australia.

Maritime Supply Chain Disruption comprise a breakdown in the distribution or flow of cargoes and their delivery to consumers using maritime and land transportations. This dimension is associated with increase freight rates, disruption of flow of government revenues, ports dues, tariffs, hold-up of import/export at ports, leading to increased lead time and costs for maritime supply chain stakeholders. Corrupted cargo reporting system also prevents safe border controls (ABF), loss of supply chain coordination and information flow, increased demurrage costs, restriction in domestic and international supply chain as well as compromised disruption Networks.

Maritime Supply Chain Disruptions and Socio Technical Disruptions were identified as the two dimensions with the most pronounced impact and greatest perceived uncertainty from cyber attacks on Australian maritime IT systems. They were thus chosen to form the foundation of the scenario.

The emergence of these two factors not only indicated a systemic issue, but also discrepancies in the ability to coordinate a response to such cyber attacks with desirable policy outcomes. There was an overall agreement that a resilient national IT system is required to prevent the occurrence of these types of attack on Australia's key maritime IT systems.

2.4.2. Impact and certainty

Positioning the five identified dimensions on the impact-certainty matrix enables a two-dimensional analysis of the severity of impact and the certainty of the impact on fuel supply chain security in the region. The disruptions-related to human issues on maritime IT infrastructure and systems were found to be relatively manageable; whilst cyber attacks will likely exert enormous impact on navigation capabilities of shipping lines and port IT systems. These disruptions and safety concerns are far more certain to occur in the immediate future, given the rapid pace of port automation and self-directed navigation. There are, however, mechanisms and international protocols for safety and security in open waters, which will help mitigate some of these risks of operational failures and safety breaches associated with cyber insecurity.

Linked to this is also the disruption of cyber-physical infrastructure which seamlessly connect and control physical assets and machinery via IT infrastructure. The cyber-enabled ships are highly vulnerable to cyber attack as they are either autonomous or remotely controlled vessels. They are interconnected cyber physical systems to perform certain key shipboard navigation and communications functions. Onboard cyber-physical systems, such as the automatic identification system (AIS), the electronic chart display and information system (ECDIS), and the global maritime distress and safety system (GMDSS), are at an elevated risk of cyber attack. Other key systems such as container tracking and Port Management Information Systems are equally at risk of failure or cyber-attack.

Socio-technical linkages will also be highly vulnerable to cyber attacks both onshore and offshore. The substructures of complex sociotechnical systems shape the perception, beliefs, and awareness of cyber security. Social aspects of human behaviour, and technical aspects of organisational structure and processes are likely to be affected by cyber threats in the Indo-Pacific region.

The Maritime Supply Chain dimension is also located in high impact-low certainty quadrant. Cyber attacks can interrupt maritime supply chains, which consist of shipping lines, port terminal operators, freight forwarders and land transport system. Increased freight rates, loss of government revenue, increased lead time, corrupted cargo reporting system, compromise in safe border controls (ABF), loss of supply chain coordination and information flow and increased demurrage costs. The minimisation of maritime supply disruptions requires the identification of critical events and associated risks, assessment of the viability of suppliers, and secure supply, and ensure the timely delivery of goods from suppliers to consumers.

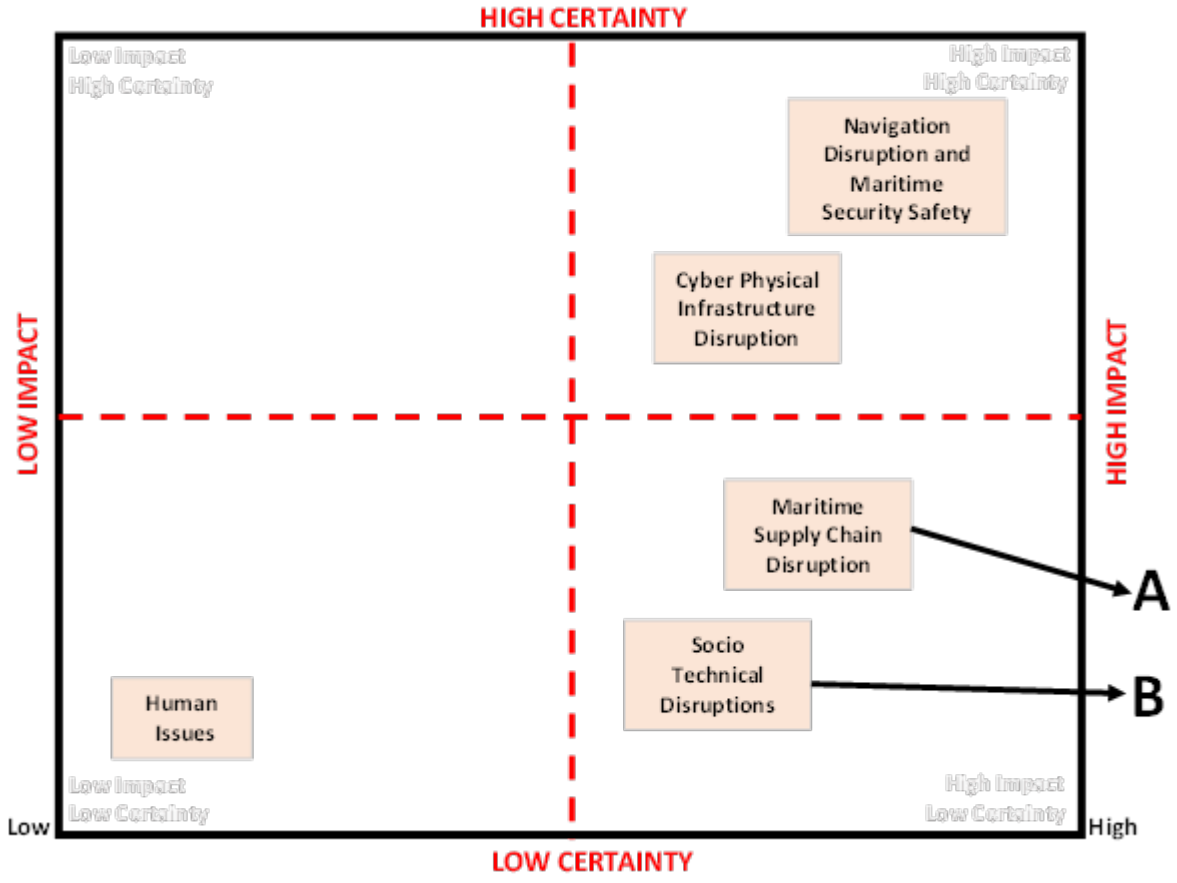


Figure 2.5: Certainty and impact of Cyber-attacks on the Australian maritime IT systems

2.4.3. Framing and scoping the scenarios

The use of a four-quadrant matrix to show Maritime Supply Chain Disruption on the vertical axis and Socio Technical Disruptions on the horizontal axis enabled workshop participants to narrate a set of extreme outcomes for each of the scenarios (i.e. Best-Best, Worst-Worst, Best-Worst, Worst-Best) as shown in Figure 2.6.

The Best-Best scenario is a situation when both Maritime Supply Chain Disruption and Socio Technical Disruptions are at their best. There will be a minimal threat of cyber attack on Australian maritime IT systems and Australia will be able to mitigate any such threat. The Best/Best scenario (quadrant 2) will produce a favourable situation to support the growth of more innovative services in Supply Chain IT services and a resilient system. This state is one where the threat of any cyber attack on Australian maritime IT systems will be reduced and there will be no delay in shipping and supply chain operations. Cyber-safe supply chain and coordination will be achieved. In this scenario, Australia will be able to develop and expand the production of alternative fuels and achieve a more innovative supply chain service based on local skills and talents.

There will also be opportunity for innovative digital ecosystems with seamless integration of Intermodal systems, more resilient future supply chains resulting from the opportunities for reconfiguration secured data protocol and risk mitigation. At the same time, delays in shipping and supply chain operations will be reduced and Australia becomes the world leader of supply chain cyber security skills and cyber safe supply coordination and collaboration.

The Worst-Worst scenario reflects the state of adversity and threat to our national resilience. It shows the likely outcomes in a state that intersect the worst of Maritime Supply Chain Disruptions and the worst of Socio-technical Disruptions. It is surmised that in the immediate future cyber attacks will have a crippling effect on maritime IT and systems, leading to multiple operational failures across the wider maritime logistics network, and malfunctioning of modal and intermodal infrastructure. This scenario will pose direct challenges such as paralysis of port gates and truck loading Infrastructure bottlenecks, congestion and delays with associated long queues at anchorages, shipping routes disruption and blockade, breakdown in ship/port automated systems, disruption to terminal operations, major spill and environmental damage, vessels unable to berth, load or discharge, and Australian maritime infrastructure completely disabled.

It is particularly more pronounced for automated or semi-automated infrastructure, which have higher reliance on IT systems. Cyber insecurity will also engender other ancillary systems such as NAVTEX (navigation telex, a unified transmission system for navigation, meteorological and other line information), AIS, radar and Global Positioning System (GPS) equipment, and other sensors supporting Internet of Things integration. This will in turn may cause operational failure, which will then directly de-stabilise socio-economic systems, create food supply uncertainty, smuggling of prohibited items, and shortage of critical components/parts. Further cascading effects will also be seen in the form of labour market disruptions, cyber skills shortage, over-regulation and government control, and increased criminality.

The Best-Worst scenario represents the best of Maritime Supply Chain Disruption and the worst of Socio Technical Disruptions (quadrant 1). Under this scenario, more cyberthreat-proofed maritime systems will be developed with unpredictable supply of essential products for national security resilience and Australian economy becomes a closed economy with a strengthening of local technology production system.

The Worst-Best scenario, quadrant 3, characterises worst of Maritime Supply Chain Disruption and the best of Socio Technical Disruptions. It is a state where the plausibility of supply chain disruptions is relatively high, but the socio-technical systems are robust to mitigate risk of cyber attacks on maritime IT infrastructure. Organisations are aware of the risks and threats of cyber attacks and emergency plans and procedures to respond to any cyber threats are clearly established. Participants are of the view that there will be inflated prices of liquid energy supplies, yet the economic impact will be minimum. Collaborative supply chains will most likely emerge to reduce increase supply chain risk through trial-and-error learning from bad experiences. Oversight regulations will be strengthened to minimise supply chain disruptions. However, institutional restructuring might occur to mitigate supply chain failure.

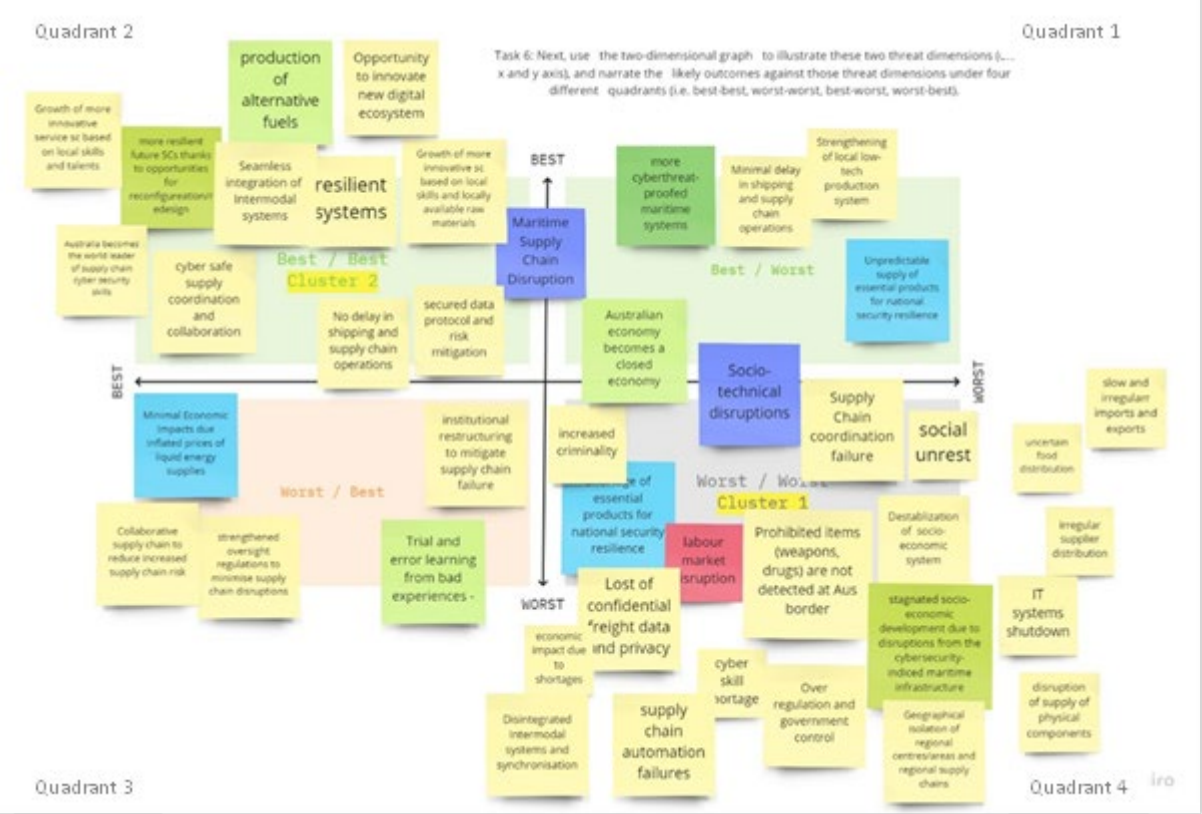


Figure 2.6: Plausible outcomes of Cyber-attack on Australian maritime IT systems

2.4.4. Plausible future outcomes

i. Australian port gates and truck-loading infrastructure will be disrupted

ii. Australian ports will be heavily congested with significant delays and long queues at anchorage

iii. Australian commercial shipping operations will be disrupted

iv. In the affected ports, vessels will be unable to berth, and load/discharge cargo

v. Access to Australian maritime infrastructure will be significantly limited

vi. Australian supply chains will be disrupted

vii. Australian Customs clearance controls may be breached

2.5. Context 3: Indo-Pacific maritime logistics network disruption

2.5.1. Key disruptions

Participants explored this context by responding to the question: 'What are the major disruptions to the Indo-Pacific maritime logistics network that are critical to Australia's maritime supply chain security?' These responses to this question were grouped and collapsed into the following dimensions:

i. Competitive Responses

ii. Disruptive Innovation

iii. Geopolitical Disruptions

iv. Ecological Disruptions

v. Trade Related Disruptions

Competitive Responses represent the consequent expected reactions of nations or organisations to strategically counter the action of other nations. Companies respond to disruptions by making decisions on reshoring, ship re-routing to find safer voyage, global port development in strategic and protected locations, or elevated security alert at ports and ships. Trade and military alliances (e.g., Quadrilateral Security Dialogue – QUAD) are other forms of competitive responses to mitigate risk of maritime logistics network disruptions.

Disruptive Innovation refers to innovations such as the Northern Sea Route, the Belt and Road Initiative, autonomous ships and automated terminals.

Geopolitical Disruptions are associated with 'political unrest and civil movements', 'political threats and conflicts', 'denial of passage through key points', and 'geopolitical imbalance'. Other disruptions have territorial elements, such as 'Hot Spots' in the Persian Gulf, Bay of Bengal, Indian Ocean, trade wars and territorial disputes, conflict in Indo-Pacific disrupting trade, and localised piracy and sabotage. Expectedly, there will be an increase in submarine activities with increased 'geopolitical alignment and network accessibility', 'conflicts in North Asia and in the Bay of Bengal', and 'militarisation of shipping routes and multimodal systems,' such as ports and airports with terrorist activity or conflict in source countries, and control and dominance of maritime infrastructure.

Ecological Disruptions are disturbing events or forces of environmental origin that cause significant disruption to maritime logistics networks and infrastructure. This dimension has clearly emerged when participants identified disruptions, such as 'pandemic', 'sea level rise - impact on port infrastructure', 'Threats on maritime infrastructure from extreme weather events' and 'climate change', 'earthquake', 'extreme weather temperature', 'heavy rain and flooding', 'destruction to major ports in the North-South route due to natural disasters' and 'epidemics and pandemics related disruptions and its impact on seafaring and shore workforce'. Other issues identified included 'maritime weather severity' and their impact on navigation routes and port access, 'hydrographic services', as well as 'size of ships versus navigable routes and port accessibility'.

Trade Related Disruption are linked to 'chokepoints', 'narrow waterways', 'high risk of collisions (e.g., Malacca Straits)', and 'major safety/security incidents on ports/ships in the North-South routes', which would then have spill-over effects, such as 'disruption to e-commerce operations', 'significant trade shrinkage', 'demand volatility and disruptions', and 'surge in demand for air transport'. 'Economic downturn', 'global fuel shortage' and 'delay in imports of critical supplies and exports of key produce' were other forms of trade-related disruptions. The unexpected slowdown of offshore supply and transhipment vulnerabilities were also identified.

2.5.2. Impact and certainty

As shown in Figure 2.7, Trade related disruptions and Disruptive innovation were identified as plausible outcomes which will be more likely to unfold for Australia in the Indo-Pacific region. As previously, a four-quadrant matrix is used, showing Trade Related Disruption on the vertical axis and Disruptive Innovation on the horizontal axis. Again, the participants narrated the storylines under each of the formulated scenarios (i.e. Best-Best, Worst-Worst, Best-Worst, Worst-Best) as shown in Figure 2.7.

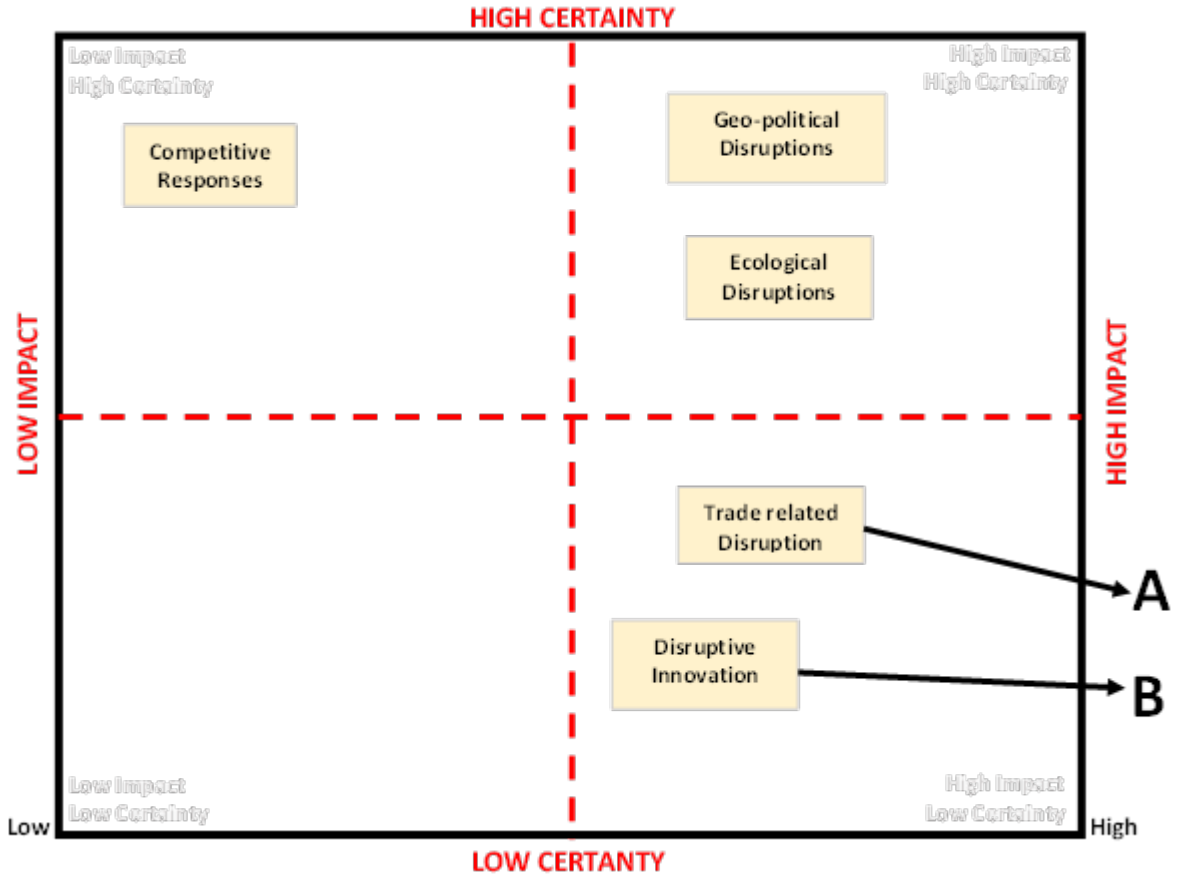


Figure 2.7: Certainty and impact of key dimensions in the context of the Indo-Pacific maritime logistics network disruption

2.5.3. Framing and scoping the scenarios

Best/Best scenario (quadrant 2) is the state when both Trade-Related Disruptions and Disruptive Innovation are at their best. Maritime logistics infrastructure will be digitally-connected systems, which will in turn minimise trade-related disruptions in the Indo-Pacific region. In this scenario, Australia will be in a better position to support a sustainable and robust economy. High-capacity logistics infrastructure will be built with the development and implementation of new business practices as well as innovative practices. Australian markets, sources and supplies will be more diversified, integrated, and adaptive to highly dynamic global production networks. Digital innovations will enable the Australian supply chains to be more resilient to absorb global shocks.

Australian supply chains will be highly competitive globally. Innovative and creative practices will also be more widely prevalent, and Australia comes out as the global benchmark. In addition, a highly capable, resilient maritime supply chain will ensure national security and robustness of the national economy. A digitally-driven radical and revolutionary approach, instead of evolutionary, will be widely

adopted to protect critical infrastructure. Enhanced IT capability and ubiquitous and highly-integrated technology will mitigate the risk of maritime infrastructure failure. Digitally-connected trade networks and efficient value chains will allow Australian Defence to anticipate threats, deploy resources in Just-in-Time and protect maritime supply chains for unplanned disruptions.

Best/Worst scenario (quadrant 1) represents a state of best of Trade Related Disruptions but the worst of Disruption Innovations. In this scenario, there will be an increased trade imbalance in favour of Australia. Trade relationships will be re-organised and new trade networks will be established with strategic partners such as the UK through perceived possibility of bi - lateral trade deals. It is expected that there will be an anachronistic systems and severe capacity constraint, and limited scale economies. At the worst of disruption innovation, there will be ageing and dilapidated maritime infrastructure, which will increase the dependence of the Australian economy on a few supportive trading partners. This disruptive innovation will cause limited supplies of power, energy, and resources, which in turn will adversely impact exports. A lack of digital innovation may lead to obsolete infrastructure which could limit the capacity of Australia to grow trade internationally. An overall reduction in standard of living for Australians may result.

Worst/Best scenario (quadrant 3) is a state that characterises the worst of Trade Related Disruptions and the best of Disruption Innovation. In this scenario, domestic consumption will be most likely to grow and economic growth will be internally driven. Australia will experience slow economic recovery with an oversupply of goods and high import costs. Poor utilisation of infrastructure and production overcapacity will reduce trade disruption. There will however be an emergence of new trade routes/alliances and development of technology - based maritime services.

Figure 2.8: Plausible outcomes different Indo-Pacific maritime logistics network disruption scenarios

Worst/Worst scenario (quadrant 4) is an apex of worst state of both Trade Related Disruptions and Disruptive innovation. Current IT systems and trade networks will be highly vulnerable to any disruption. Evolutionary or more incremental forms of digital innovations may not be able to protect severe disruption of maritime infrastructure and logistics operations. A shorter response time to market and the wider cascading impacts on the global production networks will adversely affect the ability of maritime logistics networks to recover from any perturbation. Complete stoppage of all ports and shipping operations may occur due to huge maritime trade disruptions. Extensive loss of lives and assets will result from the sudden shock and operation system failure from the use of obsolete knowledge and skills. Australia resources will be greatly depleted due to weakening Defence and National Security capabilities. Australia will witness an increased risk of service failure of maritime infrastructure. The economic and financial crisis from such worst/worst scenario will cause bottlenecks and social upheavals and economic instability in Australia.

2.5.4. Plausible future outcomes

i. The IT systems and trade networks will be disrupted.

ii. Port and shipping operations will be disrupted.

iii. Supply chain operations will be disrupted.

iv. The supplies of essential and critical goods will be disrupted or experience shortages.

v. Loss of lives and assets are caused by the sudden shock.

vi. Emergency rescue & security capabilities will be constrained and exhausted.

vii. Australia will experience an economic downturn, resulting social unrest.

3. MARITIME TRANSPORT SECURITY

3.1. Objective

The countries in the Indo-Pacific contribute 60% of global GDP with approximately 60% of global seaborne trade being transported through the region, which is home to nine out of the world's ten largest ports. One-third of global seaborne trade is transported through the SCS alone (US Department of Defense, 2019). The IPR, especially SCS and ECS, has also been challenged with increasing military presence and competition and is facing escalating maritime security threats (Tertia and Perwita, 2018). The Strait of Malacca is one of the most important shipping lanes in the world and especially for countries in South, South-East and East Asia. It carries about half of the world's oil and two-third of its liquified natural gas. The oil flow through the Strait is three times greater than through the Suez Canal and fifteen times greater than through the Panama Canal (Khurana, 2004).

In terms of volume, more than 99% of Australia's international trade is carried by sea. In 2019, Asia contributed 65.7% to Australia's two-way trade value, equivalent to 32% of Australian GDP in the same year. Four of Australia's five largest trading partners are in Asia (Department of Foreign Affairs and Trade, 2020). Therefore, disruption of maritime transport in the region could cause very significant disruption to Australia's trade and national economy (Department of the Environment and Engery, 2019, Gallagher, n.d.).

The main objective of this study is to gain a better understanding of the vulnerability of Australian fuel supply chains to disruption of shipping operations in the region, given the fact that Australia imports about 69% of crude oil and 58.2% of product oil for domestic consumption (Department of Industry, 2021). To achieve this objective, an analysis of the Indo-Pacific maritime network was conducted to study the structure and connectivity of the maritime network and its role in Australian fuel supply chains, and to show how disruption to this network may impact on Australia's trade, especially fuel imports that are critical to the national security and economy.

Figure 3. 1 : Selected Indo-Pacific maritime security incidents, 2001-2011 (Medcalf et al., 2011)

The study also provides a scenario analysis of maritime security threats in the SCS and the ECS to countries in the region and a discussion of the strategic policy implications for Australia. The SCS and

ECS are chosen because they are not only critical to maritime supply chains in the Indo-Pacific but have also been subject to a number of maritime security incidents as illustrated in Figure 3.1 (Medcalf et al., 2011, Tertia and Perwita, 2018).

3.2. Data set and study method

The study used AIS data on vessels' details, loading condition, and departure and destination ports collected from Marine Traffic; and data on Australian energy supplies and trade from Department of Industry, Science, Energy and Resources (2021) and British Petrol (BP, 2021). AIS data on tanker sailings in the Indo-Pacific were collected for an approximate six-week period from early August to late September 2021. The tanker sailing data set covers the network of 996 voyages in the Indo-Pacific and Middle East regions available on Marine Traffic.

The analysis is conducted in four main steps. In the first step, AIS data are used to explore Australia's port-to-port energy seaborne trade with other countries in the Indo-Pacific. The AIS data sample is also used to identify Australian ports involved in Australian seaborne energy trade within the Australian tanker network. In the second step, using various measures at the network and node levels, this study compares Australian tanker network with the Indo-Pacific tanker network to gain an insight into the role of the latter in Australia's fuel supplies.

In the third step, Australia's fuel import chains are mapped to gain a further insight into the vulnerability of Australia's fuel supply chains. The mapping also supports the fourth step, which includes a scenario analysis of maritime security threats in the SCS and ECS and discussion of policy implications for Australia. Considering the maritime security threats in SCS and ECS as shown in Lowy Institute (2021), a scenario of the closure of these waters to international shipping is considered. The closure of these waters has a significant impact not only on Australia's fuel exports and imports, but also on global shipping operations and countries such as Japan as a main liquid fuel supplier for Australia. Re-routing to avoid these regions is considered and the distance for sailing from the Middle East to the Far East for the new route is calculated. The implications for the tanker network and energy security management are then discussed and used as inputs for policy study.

In this study, the *Australian tanker network* refers to the network of those countries/ports that *directly* trade with Australian and therefore are critical to the Australia's economy and security. It is derived from tanker voyages that have their departure or destination ports in Australia. *The Indo-Pacific tanker network* refers to the network of tanker sailings in the Indo-Pacific *and* Middle East. The Middle East oil exporting countries are included in the analysis because of their critical role in the world's fuel supplies. For example, interruptions to tankers transporting crude oil from the Middle East to Japan are expected to affect the operations of refineries in Japan. Such interruptions would have an indirect impact on Australia's energy supplies imported from Japan. However, such interruptions cannot be analysed using the Australia tanker network because this network does not cover tanker voyages between Japan and the Middle East.

The comparison of the two networks is carried out using port-level and network-level measures. The port-level measures include the connection degree, betweenness and closeness centrality, and the network-level measures include the following[2]:

I. Average path length
II. Clustering coefficient
III. Density
IV. Diameter

[2] See Kanrak et al. (2019) and references thereof for more detail.

V. Average degree centrality
VI. Average betweenness centrality
VII. Average closeness centrality

3.3. Findings on maritime transport and critical supply security

3.3.1. Australian tanker network

Australia is involved in both importing and exporting fuel from countries in the Indo-Pacific. The data shows Australia mainly imports crude oil and oil products, and exports LNG and LPG. Tables 3.1 and 3.2 show the foreign ports that Australia imports from or exports to. These are the foreign ports that have direct maritime trade links with Australian ports. Table 3.1 shows the Australia inbound tanker sailings from eight countries covered by the data set, namely Brunei, Indonesia, Japan, Malaysia, New Zealand, Singapore, Taiwan (China) and Thailand. Australia imports fuel through Adelaide, Brisbane, Darwin, Geelong, Gladstone, Kwinana, Melbourne, Newcastle, Port Hedland and Townsville. It is interesting to note there is no sailing from the Middle East to Australia identified by the data.

Table 3.1: Australia inbound tanker sailings

Departure country	Foreign Departure port	Australian destination port
Brunei	Muara	Gladstone
Brunei	Muara	Kwinana
Brunei	Muara	Kwinana
Brunei	Muara	Port Hedland
Indonesia	Ciwandan	Gladstone
Japan	Himeji	Darwin
Malaysia	Tanjung Pelepas	Geelong
New Zealand	Dunedin	Kwinana
New Zealand	New Plymouth	Melbourne
New Zealand	Tauranga	Kwinana
Singapore	Singapore	Adelaide
Singapore	Singapore	Brisbane
Singapore	Singapore	Melbourne
Taiwan	Mailiao	Newcastle
Taiwan	Yung An	Darwin
Thailand	Rayong	Geelong
Thailand	Rayong	Geelong
Thailand	Rayong	Townsville

Table 3.2 shows the outbound tanker sailings reflecting Australian energy exports especially gas fuel to Japan, Malaysia, New Zealand, Philippines, Singapore, Taiwan (China), US and Vietnam. The data indicates that **countries that have two-way fuel trade with Australia are Japan, Malaysia, Malaysia, Philippines and Taiwan (China)**.

Table 3.2: Australian outbound tanker sailings

Australian departure port	Foreign Destination port	Destination country
Botany	Lyttelton	New Zealand
Brisbane	Batangas	Philippines
Brisbane	Singapore	Singapore
Darwin	Sakai	Japan
Darwin	Shibushi	Japan
Darwin	Shimizu	Japan
Darwin	Yokohama	Japan
Darwin	Chiba	Japan
Darwin	Ho Chi Minh	Vietnam
Fremantle	Pasir Gudang	Malaysia
Geelong	Mailiao	Taiwan
Gladstone	Bluff	New Zealand
Ichthys Venturer	Singapore	Singapore
Melbourne	Bluff	New Zealand
Townsville	Seattle	US

The following notes can be drawn from the above:

i. **The energy trading partners listed in Tables 3.1 and 3.2 are in close proximity to Australia. This reflects the distance or 'gravity' effect**[3]. Because of the high freight cost relative to the cargo value, sailing distance has an important effect on energy trade. A change to sailing distance by tankers is expected to have a direct negative impact on fuel price and supplies in the global market.

ii. **Because of their direct involvement in Australian energy supplies, disruption of the energy supply chains of the oil product exporting countries will affect Australian energy supplies**. The next section reveals the fuel maritime supply chains that are important to Australia's energy trading partners in the Indo-Pacific.

[3] The gravity theory of trade proposed by Isard (1954) and Tinbergen (1962) suggests bilateral trade between any two countries depends on the distance between them and the size of their economies, similar to Newton's law of gravity.

3.3.2. Indo-Pacific tanker network

The Indo-Pacific tanker network is covered by a data set of 996 voyages in the Indo-Pacific and Middle East regions. This network covers 306 ports across 33 countries in the Indo-Pacific and Middle East regions. Table 3.3 lists the countries in the Indo-Pacific and Middle East tanker network with the number of the port and sailings in the studied network. The second column shows the distribution of ports across the countries. Most are in the Indo-Pacific. The US has the largest number of ports (45), followed by Indonesia (36), India (26), Japan (25), Malaysia (22) and Australia (17), the Philippines (16), United Arab Emirates (UAE) (14), Saudi Arabia (12) and Vietnam (11). In this report, Taiwan refers to Taiwan (China).

Table 3.3: Data Sample for the Indo-Pacific Middle East Tanker Network

Country	Number of ports	Number of voyages to or from the country	Percentage
United Arab Emirates	14	197	13.1%
Malaysia***	22	168	11.2%
Indonesia*	36	144	9.6%
Singapore***	1	133	8.9%
India	26	124	8.3%
Saudi Arabia	12	90	6.0%
United States**	45	84	5.6%
Australia	**17**	**65**	**4.3%**
Japan***	25	58	3.9%
Taiwan***	7	58	3.9%
Iraq	3	49	3.3%
Oman	7	43	2.9%
Vietnam**	11	38	2.5%
Philippines**	16	37	2.5%
Qatar	3	34	2.3%
Bangladesh	2	33	2.2%
Kuwait	4	31	2.1%
Yemen	4	28	1.9%
Myanmar	4	14	0.9%
Brunei*	1	12	0.8%
New Zealand***	8	12	0.8%
Bahrain	2	9	0.6%
Iran	9	7	0.5%
Cambodia	2	5	0.3%
Jordan	1	5	0.3%
Sri Lanka	2	5	0.3%
Papua New Guinea	4	4	0.3%
Thailand*	9	4	0.3%
Cyprus	2	3	0.2%
Israel	2	3	0.2%
Lebanon	2	3	0.2%
Syria	1	1	0.1%

Note: * - Countries with sailings to Australia
** - Countries with sailings from Australia
*** - Countries with sailing to and from Australia

The last two columns of Table 3.3 show the number of voyages *to* or *from* the countries to other countries in the Indo-Pacific and the Middle East. It shows the contribution of each country to the tanker operations and their reliance on maritime transport for their fuel supplies. Of the total of 1501 voyages *to* or *from* the countries[4], about two-thirds (67%) are international voyages and one-third (33%) is coastal voyages. It shows the importance and domination of UAE with 197 voyages (13%), Malaysia 168 (11%), Indonesia 144 (10%), Singapore 133 (9%), and India 124 (8%) in the Indo-Pacific tanker network. The remaining countries in the top ten in terms of the number of voyages are Saudi Arabia 90 (6%), the US 84 (6%), Australia 65 (4%) and Japan 58 (4%). There is *no* association between the number of ports and number of voyages indicated by the data. Despite having only one port, Singapore ranks 4th in the group of 32 countries. Australia is in the top ten countries in the list in terms of the number of ports and the number of voyages.

Table 3.3 also shows that most countries in Australia's fuel supply chains have active tanker operations with a relatively large number of sailings in the network. These are Malaysia, Indonesia, Singapore, the US, Japan, Taiwan (China), Vietnam and the Philippines.

Table 3.4 presents the key measures of the Australian and Indo-Pacific tanker networks. It indicates the Australian tanker network with 44 ports and 55 links is much smaller than the Indo-Pacific network with 441 ports and 1492 links. This implies the Australian tanker network would have less exposure to tanker operation disruptions and maritime security issues than the Indo-Pacific network.

The Australian tanker network has a much smaller measure of average betweenness centrality but higher density measure than the Indo-Pacific network. The other measures including the average path length, clustering coefficients and density are relatively comparable.

Table 3.4: Indo-Pacific and Australian tanker networks

Network properties	**Indo-Pacific tanker network**	**Australian Network**	
		Entire tanker network	Fully/partially loaded tanker network
Number of ports	441	44	38
Number of links	1492	55	42
Average path length	3.786	3.263	2.516
Clustering coefficient	0.164	0.112	0.028
Density	0.008	0.029	0.030
Diameter	11	9	8
Average degree centrality	6.766	2.5	2.211
Average betweenness centrality	737.149	20.205	7.553

[4] The sum of the numbers of voyages across the countries (1,501) is larger than the total number of voyages (996) covered by the data set because the former 'double-counted' cross-countries voyages.

Average closeness centrality	0.00002	0.00069	0.0083

3.3.3. Australia's petroleum maritime supply chains

AIS data on tanker sailings in the Indo-Pacific, collected for an approximate six-week period from early August to late September 2021, were used to map Australian maritime supply chains. The mapping covers not only Australia's petroleum imports from exporting countries but also their countries' imports from third countries. For the purpose of analysis of Australia's energy security, the main focus is on Australian imports of petroleum.

Figure 3.2 shows the maritime supply chains that Australia relies on for petroleum imports from Brunei, Indonesia, Japan, Malaysia, New Zealand, Singapore, Taiwan (China) and Thailand. It also shows how these countries rely on third countries for their fuel production and consumption. Note some of these countries also import from Australia. The AIS data shows Australia mainly imports oil products from oil-product exporting countries, which import crude oils from other countries.

There are four levels of impacts on Australian maritime supply chains as shown in Figure 3.2:

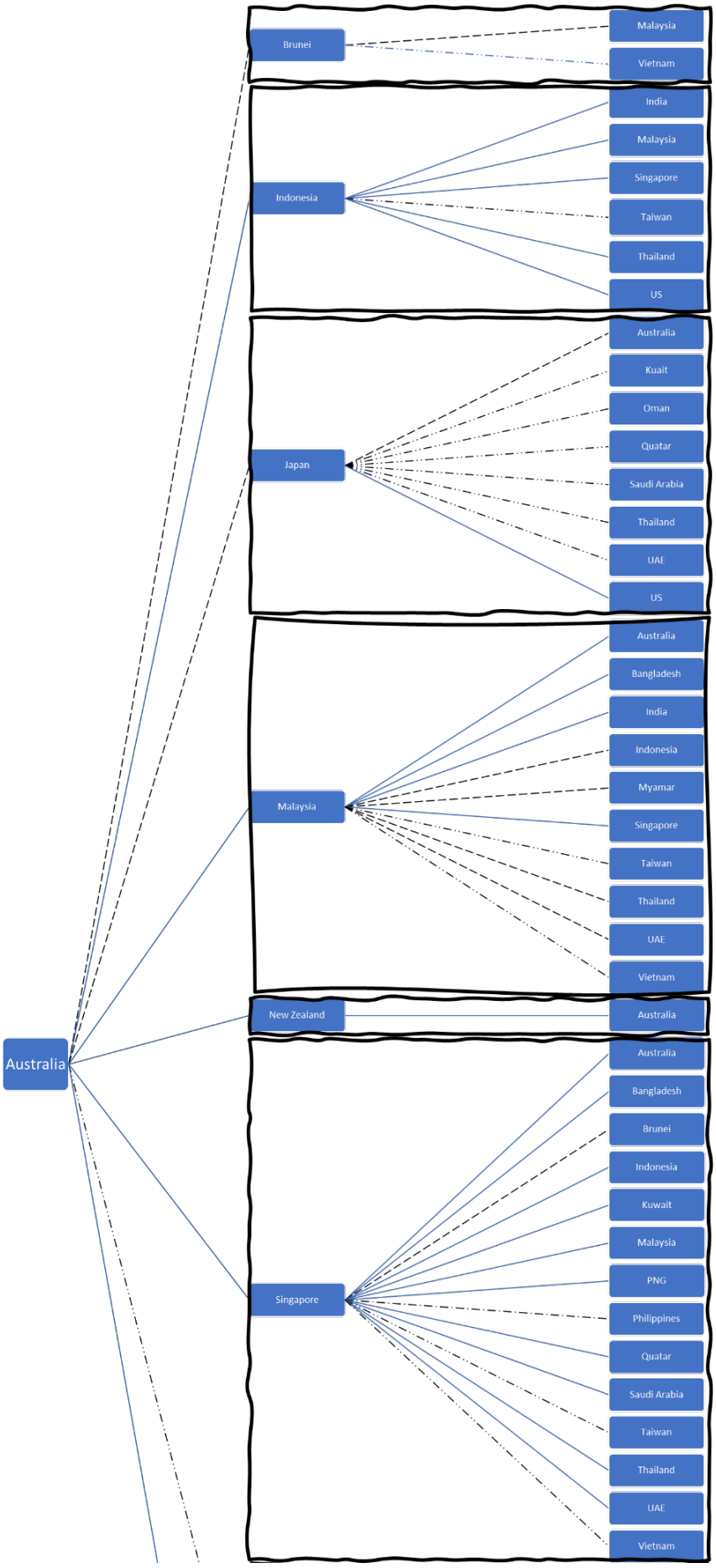
i. No or a very low impact is shown by solid lines (———), e.g. shipping between Australia and New Zealand.

ii. Low impact shown by dash lines (- - - - - - - -) where shipping to/from some ports in the country is affected by the study scenario, e.g. shipping between Malaysia and Thailand.

iii. Medium impact is shown by single dot dash lines (- · - · - · -) where shipping to/from many ports of the country is affected and significant rerouting is required, e.g. shipping between Singapore and the Philippines.

iv. High level of impact shown by double dot dash lines (– · · – · · –) where most ports of the country are affected, e.g. Vietnam and Taiwan (China), or vessels' rerouting would extend the distance very significantly, e.g. shipping from the Middle East to Japan (further discussed below).

As shown in Figure 3.2, Australia's imports are transported from eight countries (Brunei, Indonesia, Japan, Malaysia, New Zealand, Singapore, Taiwan (China) and Thailand). Shipping from Indonesia, Malaysia, New Zealand, Singapore, and Thailand to Australia is not affected by the sea closure. Only Taiwan (China) will be very significantly impacted by the sea closure, while the impact on shipping from Japan and Brunei to Australia is low. If Bruneian ports are still accessible, the shipping distance from this country to Australia will not be significantly affected. Similarly, direct shipping from Japan to Australia will be subject to only a relatively low impact.


Australia
Brunei
Malaysia
Vietnam
Indonesia
India
Malaysia
Singapore
Taiwan
Thailand
US
Japan
Australia
Kuait
Oman
Quatar
Saudi Arabia
Thailand
UAE
US
Malaysia
Australia
Bangladesh
India
Indonesia
Myamar
Singapore
Taiwan
Thailand
UAE
Vietnam
New Zealand
Australia
Singapore
Australia
Bangladesh
Brunei
Indonesia
Kuwait
Malaysia
PNG
Philippines
Quatar
Saudi Arabia
Taiwan
Thailand
UAE
Vietnam

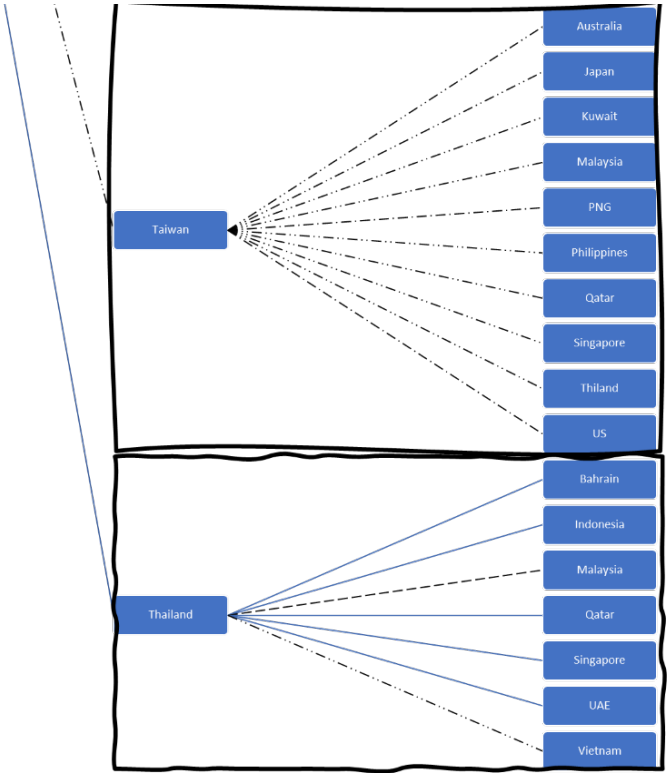


Figure 3. 2: Australia's petroleum maritime supply chains

However, there is a high level of interdependence between countries in fuel supply chains, e.g. Australia imports product oil from Japan, which imports crude oil from Saudi Arabia and Thailand. Therefore, an impact on maritime transport and production upstream in the supply chain from Japan would have an impact downstream. Although the data set does not capture tanker sailings to or from other countries in North Asia, a similar impact on supply chain from this region is expected. Given the fact that 32% of Australia's oil product is imported from Japan and South Korea, of which 87% and 81% of crude oil imports respectively are sourced from the Middle East (Department of Industry, 2019), the result implies a significant impact on Australia liquid fuel supplies.

3.3.4. Impact of SCS and ECS maritime security threats

This section presents a scenario of maritime security threats in SCS and ECS, similar to the scenario setting explained in Akimoto (2017). Confrontation between China and other littoral nations in SCS has been increasing in recent years with intensifying 'grey zone' activities and fears of open conflict. China declares the waters inside the nine-dash line a 'denial area'. This area, as claimed by China, is vaguely described by diagram without precision, and varies over time in response to dynamic claims. China claims that all foreign vessels require China's permission for innocent passage in the waters inside the nine-dash line because such waters are under China's sovereignty or are territorial seas with respect to claims landmasses inside the nine-dash line. In response to the situation, the US deploys naval forces in the Western Pacific Ocean. US navy forces persist with exercising freedom of navigation and the right of innocent passage along SLOCs throughout the SCS, ignoring China's request for obtaining approval. This results in rising tensions between the US and China, with increasing non-combat naval interactions, 'warnings off', and media rhetoric. China also warns foreign tankers not to enter the area, under the pretext of preventing environmental contamination, arguing that if a large oil tanker were accidentally attacked and an oil spillage were to take place, the marine environment would be severely damaged. China also announces that, if US forces take more assertive action, China

will respond with anti-access operations in the sea area between the first and second island chains. The ECS is the sea in the northern Pacific Ocean bounded by China, Japan, the Ryukyus, and Taiwan. This area is subject to dispute between Japan and China over the Senkaku/Diaoyu Islands that are covered by the US-Japan Security Treaty (Panda, 2014). This sea has seen a more frequent presence of China Coast Guard vessels in the contiguous zone of the Senkaku/Diaoyu Islands (Mochizuki and Han, 2020). The tensions have also been increasing as in November 2021, China held live-fire military drills in ECS (Wang, 2021). The scenario is limited to the closure of SCS and ECS, which have seen many military incidents (see Figure 3.1 above) and have a potential impact on shipping activities in the region. This extends to maritime security between first and second island chains and requires rerouting of vessels via the Torres Strait or Bass Strait.

Figure 3.3 illustrates the current major crude and product oil trade flows in SCS and the critical role of this sea in fuel energy security for countries in Southeast and North Asia. Shipping connecting Australia to East Asia is via Lombok Strait (Indonesia). It implies the closure of SCS will have a critical impact on shipping activities and energy supplies in the region. However, the impact varies among the countries depending on:

I. the extent to which the country relies on this sea for their maritime transport
II. the availability of and access to alternative routes.

The closure of the SCS and ECS will likely impact countries that rely on SCS for their exports and imports.

Figure 3. 3: Major Crude Oil Trade Flows in South China Sea (Hirst, 2014)

As indicated by Figures 3.2 and 3.3, all shipping routes connected to Taiwan will be directly impacted and all imports to Brunei will also be affected. Seven out of eight shipping routes to Japan are affected and six of them are subject to a very significant impact. Six out of ten shipping routes to Malaysia, four out of fourteen routes to Singapore, and two out of seven routes to Thailand will be affected.

The closure of the SCS will force shipping lines to reroute their vessels potentially via the Sunda Strait and Lombok Strait (Akimoto, 2017). For illustration, Table 3.5 and Figure 3.4 show the waypoints of the alternative route connecting North Asia to the Laccadive Sea via the Sunda Strait to avoid the SCS. Avoiding the SCS and ECS adds 883 nautical miles to the voyage or 14% to the sailing distance and time for a one-way voyage from the Middle East to East Asia. Calculated for an average vessel speed of 12 knots, this adds about three days. Increasing the speed to avoid delay would increase fuel consumption exponentially[5]. The most direct impact of longer sailing distance and voyage time is an inflation of the freight rates and shipping costs. For example, the on-going Russia trade sanction and Russia-Ukraine war have resulted in the tanker freight rates in spot markets increased by 345% (Bockmann, 2022).

Table 3.5: Waypoints of alternative route between North Asia and Middle East

No.	Name	Lat	Lon	Crs	Dist	TDist
1		05°39.120'N	078°05.186'E	114.7	1607.9 NM	0.0 NM
2		05°46.039'S	102°21.219'E	106.8	138.2 NM	1607.9 NM
3		06°25.807'S	104°34.165'E	082.6	37.9 NM	1746.1 NM
4		06°20.908'S	105°11.837'E	083.3	21.0 NM	1784.0 NM
5		06°18.424'S	105°32.971'E	033.1	44.5 NM	1804.9 NM
6		05°40.788'S	105°57.451'E	105.8	36.6 NM	1849.5 NM
7		05°50.755'S	106°32.733'E	068.1	12.5 NM	1886.1 NM
8		05°46.127'S	106°44.207'E	074.8	20.9 NM	1898.6 NM
9		05°40.613'S	107°04.442'E	084.8	316.1 NM	1919.5 NM
10		05°11.868'S	112°20.046'E	095.0	57.3 NM	2235.5 NM
11		05°16.907'S	113°17.248'E	091.5	228.5 NM	2292.8 NM
12		05°22.975'S	117°06.513'E	037.0	134.9 NM	2521.4 NM
13		03°34.741'S	118°27.696'E	001.5	56.6 NM	2656.2 NM
14		02°37.957'S	118°29.183'E	017.6	230.1 NM	2712.8 NM
15		01°02.572'N	119°38.623'E	055.4	312.4 NM	2942.9 NM
16		04°00.749'N	123°55.486'E	058.5	108.4 NM	3255.3 NM
17		04°57.619'N	125°28.111'E	045.8	119.8 NM	3363.8 NM
18		06°21.566'N	126°54.383'E	017.5	604.2 NM	3483.6 NM
19		15°59.733'N	130°01.585'E	359.7	590.5 NM	4087.8 NM
20		25°52.240'N	129°58.606'E			4678.3 NM

The impacts of SCS and ECS closures on Australian fuel imports would be a combination of the following:

i. Rerouting to avoid the conflict/affected areas that will extend *sailing distance* and *voyage time* very significantly across all shipping sectors.
ii. Longer sailing distance due to (i) directly increasing tanker freight rates.
iii. Longer voyage time due to (i) directly increasing demand for tankers thereby further increasing tanker freight rates.
iv. Global shipping market freight rates increasing significantly across all shipping sectors because of (i) and (ii).
v. (iii) will cause a severe shortage of crude oil supply for refineries in affected countries such as Japan and Korea.
vi. Fuel supply shortage due to (v) further increasing global market freight rates and supply costs.

[5] Increasing the tanker speed reduces vessel voyage time but increases fuel cost very significantly. The relationship between actual fuel consumption and speed can be approximated by the formula: $F_a = F_0 \left(\frac{S_a}{S_0}\right)^{\alpha}$, where F_a - actual fuel consumption, S_a - actual speed, S_o - design, optimal speed, F_o - fuel consumption at the optimal speed, α - coefficient depending on various other factors e.g. engine design and technologies, ship hull and sea conditions. For $\alpha = 3$, an increase in the vessel speed by five knots from 12 to 15 knots would nearly double fuel consumption and an increase to 17 knots would increase fuel consumption by 2.8 times.

vii. Many countries with control and ownership of the tanker fleet may take action to keep tanker service for their own use because of (ii)-(vi).

viii. Global market freight rates will increase even further because of (vii)

ix. Fuel supply shortage across countries including Australia will be further worsened because of (vi) and (viii).

x. Fuel price in across countries including Australia will increase substantially because of (ix).

xi. Global supply chains will be disrupted because of (i) and (x).

xii. Production costs and prices of goods e.g. sea foods, agricultural and mineral products, and services e.g. air transport, taxi, courier services, will also increase substantially, because of (x) and (xi).

xiii. (x)-(xii) will cause economic recession, hyperinflation, high unemployment, and social unrest across Indo-Pacific countries including Australia.

xiv. Because of (xiii), many countries in the Indo-Pacific may determine to take action and join international coordination to protect their fleet, seaborne trade and to ensure freedom of navigation in the SCS and ECS.

xv. Alternative to (xiv), countries may take action early from the outset instead of waiting until (xiii) happens.

xvi. (xiv) or (xv) may ultimately lead to armed conflicts in the SCS and ECS.

xvii. (xvi) may cause severe social, economic and environmental impacts and loss of lives in the SCS, ECS or the broader Indo-Pacific region.

xviii. Because of (xiv) or (xv) and or (xvi) Australia may join allies and other countries in the region to ensure the Freedom of Navigation Operations (FONOPS) and uphold the rules-based international maritime order.

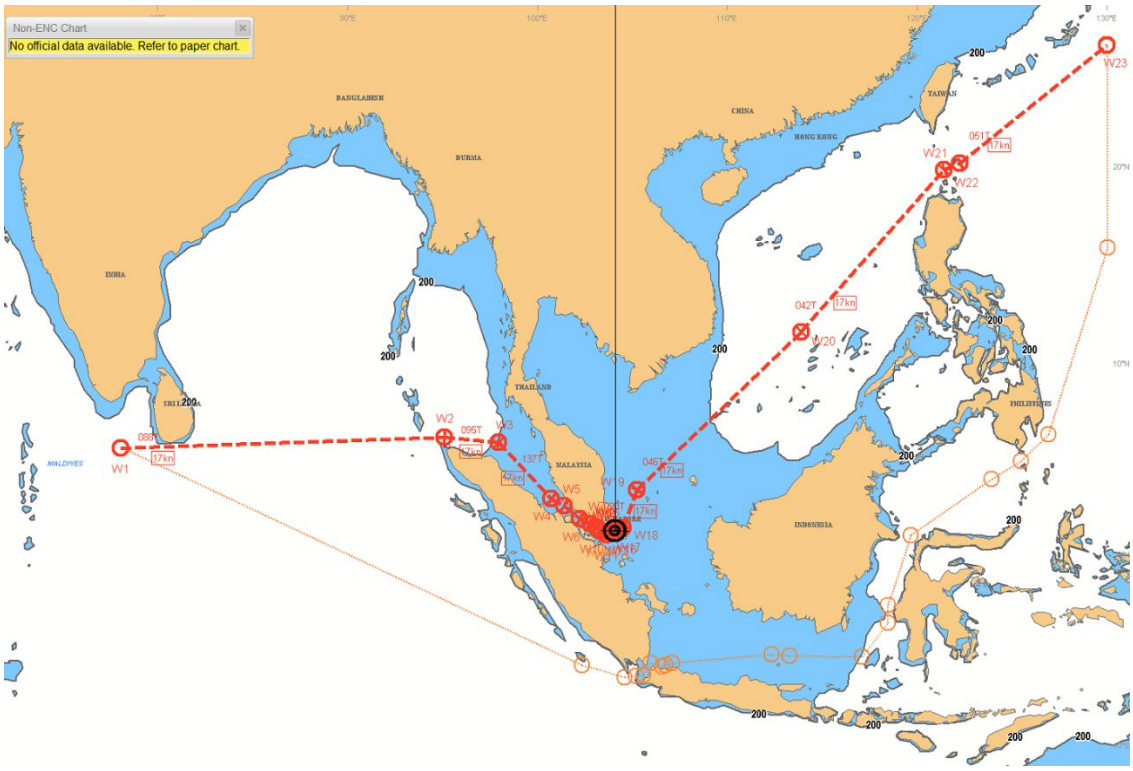


Figure 3. 4: Alternative route between North Asia and Middle East

3.4. Implications

The scenario analysis in the previous section shows the extensive impacts and consequences of maritime security threats in the SCS and ECS on the IPR. The analysis focused mainly on the tanker network and fuel supply chains. Similar analyses can be conducted for export and import chain of other commodities. The impacts identified by the study give rise to a range of strategic options for the Government, from (1) do nothing, (2) wait and see, (3) observe and monitor, (4) be prepared, to actively minimise the maritime security threats. One option is to minimise reliance on imports. This means domestic production capacity should be increased. This at best results in a self-sustained economy and helps to minimise external impacts. Alternatively, to minimise reliance on any single country, Australia can produce sovereign goods domestically or choose to import only from allies, diversify supply sources, and maintain a strategic fleet to control the supply chains.

It is clear that one of the key issues is to choose among strategic directions. Two of the most notable are: (i) to look inward and focus on developing a self-sustainable economy, and (ii) to look outward and take a proactive approach to economic development balanced between trade and domestic production. This choice requires the following consideration of Australia's strategic position.

First, despite the impact of the global pandemic, global supply and logistics chains continue their indispensable role in mobilising resources, transferring technologies and allowing countries to support each other. Well-managed global trade and supply chains would make the world safer and more resilient to disruption.

Second, the social-economic and geo-politic landscape has been changing quickly with international competition. Table 3.5 shows the power indexes of countries with their interests in the Asian region calculated by the Lowy Institute (2021) using 131 indicators across eight areas, military capability and defence networks, economic capability and relationships, diplomatic and cultural influence, resilience and future resources. It indicates that the US and China are by far the most influential countries in the group of 26 countries studied.

Third, it follows from the above that small countries in the Indo-Pacific will inevitably be affected by influential countries. Alternatively, they face the risk of isolation and being left side-lined.

Fourth, global issues require global leadership and global partnership. This is especially true when it comes to resolving the increasing tension and territorial disputes in the region. On the other hand, global demand for energy keeps increasing due to growing population and human consumption, while resources become scarce, and cost of exploration and mining will increase. This creates pressure for the use of the ocean and worsens maritime territorial disputes.

Fifth, Australia and New Zealand are the only two western democratic countries in the East. Australia has the largest land size and ocean resources in the Indo-Pacific and has the largest economy compared with the neighbouring countries.

Considering the above, it is apparent that the Australia, its land and ocean resources, and seaborne trade need to be protected. Australia needs to take a leadership role in the region and work with its allies and friends to protect its interest and uphold the rules-based international order. The recent changes in the Australia-China relationship (Jain, 2021) and Solomon Islands' strategic direction (Meg Keen, 2021) are examples of the importance of Australia's influence.

Table 3.6: Asia Power Index 2021

Country	Rank	Score	Group
US	1	82.2	Super powers ≥ 70 points
China	2	74.6	Super powers ≥ 70 points
Japan	3	38.7	Middle powers ≥ 10 points
India	4	37.7	Middle powers ≥ 10 points
Russia	5	33.0	Middle powers ≥ 10 points
Australia	6	30.8	Middle powers ≥ 10 points
South Korea	7	30.0	Middle powers ≥ 10 points
Singapore	8	26.2	Middle powers ≥ 10 points
Indonesia	9	19.4	Middle powers ≥ 10 points
Thailand	10	19.2	Middle powers ≥ 10 points
Malaysia	11	18.3	Middle powers ≥ 10 points
Vietnam	12	18.3	Middle powers ≥ 10 points
New Zealand	13	17.8	Middle powers ≥ 10 points
Taiwan	14	16.2	Middle powers ≥ 10 points
Pakistan	15	14.7	Middle powers ≥ 10 points
Philippines	16	13.1	Middle powers ≥ 10 points
North Korea	17	11.5	Middle powers ≥ 10 points
Brunei	18	9.6	Minor powers < 10 points
Bangladesh	19	9.4	Minor powers < 10 points
Sri Lanka	20	8.6	Minor powers < 10 points
Myanmar	21	7.4	Minor powers < 10 points
Cambodia	22	7.1	Minor powers < 10 points
Laos	23	6.0	Minor powers < 10 points
Mongolia	24	5.7	Minor powers < 10 points
Nepal	25	4.5	Minor powers < 10 points
Papua New Guinea	26	3.7	Minor powers < 10 points

Source: Adapted from Lowy Institute (2021)

White (2021) provides a perspective on Australia's capability to protect its seaborne trade. It is important to note that although Australia has a vast land size and ocean, we are constrained by a relatively small armed force, population and economy. To protect the country, land and ocean resources and trade, Australia must develop a highly capable, modern, efficient defence system. The following are recommended for defence development and further policy recommendations are provided in Section 5.

i. Build strong partnerships and develop and maintain regional cooperation with allies, neighbours and other countries in the IPR
ii. Use UAVs and drones for sea petrol
iii. Promote a strong relationship between the defence, especially navy and maritime industries
iv. Extend the coast guard capacity
v. Develop, construct and support the use of advanced technologies e.g. automated, unarmed vehicles, IT capabilities, alternative energy technologies
vi. Develop a highly integrated and coordinated defence system
vii. Develop a world-class armed force, with a focus on recruitment, university scholarships and an increase in army reserve capacity
viii. Develop an 'transformable' army that can combat during wars and build during peace

4. MARITIME CYBER SECURITY

4.1. Overview

Cyber security is a major and growing issue for Australian maritime logistics networks. According to the Australian Cyber Security Centre (ACSC, 2021), there were over 67,500 cybercrimes reported in Australia in 2020-2021, an increase of nearly 13% from 2019-2020. Self-reported loss from cybercrime was more than $AUD 33 billion (ACSC, ibid). Knowledge about the impact of cyber-attacks on maritime logistics networks however is limited, highly fragmented and anecdotal (Karahalios, 2020). An analysis of cyber security risks and threats to maritime logistics networks in Australia is needed to help execute informed decisions on protected borders, securing shipping routes, and safeguarding Australia's interest in the Indo-Pacific region.

Cyber threats are regarded by the International Maritime Organisation (IMO) as "malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions)" (IMO, 2017, p.2). These actions either target key system vulnerabilities, for example outdated software or ineffective firewalls, or exploit a vulnerability in operational or information technology. When vulnerabilities in systems are exposed or exploited directly (such as mail servers, for example Microsoft Exchange) or indirectly (such as information leakage), they may then lead to loss of control, system failure and shutdown, information leakage linked to breach of data confidentiality, or a compromise on the safety of bridge navigation or main propulsion systems. Furthermore, cyber threats or cyber risks are intangible; hence, their consequences are also intangible; and they are often difficult to detect (Karamperidis et al., 2021). When an incident occurs, its consequences might extend from a single event to a global supply chain disruption. When the 220,000-tonne 'Ever Given' vessel became stranded in the Suez Canal in March 2021, shipping was delayed for more than 6 days. This is an example of how a damaged ship (not cyber related) could globally impact the maritime industry.

Cyber-attacks on maritime logistics networks can be either targeted where a company or a ship's systems and data are the intended targets or untargeted, where a company or a ship's systems and data are one of many potential targets (BIMCO, 2021). In addition, systems can also be the intended target where the cyber breach comes from intentional malicious actions or the unintended target where the breach is an effect of negligence or ignorance (Lagouvardou, 2018, p.45) as reflected in Table 4.1.

Table 4.1: Types of Cyber Attacks (adapted from Lagouvardou (2018))

	Intended	**Unintended**
Targeted	Brute force Distributed denial of service Spear-phishing Subverting the supply chain Network port scanning	Falling victim to social engineering Unknown vulnerabilities in systems or applications System or application failure
Untargeted	Malware Phishing Water holing Scanning	User error

Among various types of cyber-attacks elaborated in Table 4.1, malware and distributed denial of service (DDoS) are becoming commonplace in the maritime industry. Malware attacks often introduce malicious programs or codes, including network outages and data infiltration, to block access to maritime corporate systems or disable ship-based systems (Kuhn et al., 2021). Some malware attacks also focus on data theft such as the theft of personal and business data. These cyber-attacks can cause supply delays and disruptions to land and sea operations (Kuhn et al., 2021). An example of such a malware attack befell the giant global shipping company Maersk in 2017. Ransomware known as 'NotPetya' was introduced into Maersk's computer-based applications and servers across 600 sites across 130 countries (Palmer, 2019). Nearly 50,000 infected endpoints such as Maersk servers and laptops were badly infected including Maersk's laptops sporadically restarting, banks of desktop screens shutdown and physical access gates were locked and corporate phones stopped working (Palmer, 2019). As a result, Maersk's port terminal operations ground to a halt and Maersk ships stood stagnant at sea. It was estimated that this attack cost Maersk US$300 million in lost revenue, information technology restoration, and operational costs (Sadek, 2021).

DDoS, where the perpetrator(s) attempt to overwhelm targeted servers or its surrounding network infrastructure with a flood of internet traffic (Karahalios, 2020), is also becoming a common occurrence and can have far-reaching consequences. For example, in October 2018, the port of Vancouver suffered a DDoS attack which led to 225,000 user accounts being impacted (Nicaise, 2021).

Historically, maritime-based cyber-attacks have focused on ship navigation systems, where the perpetrators introduce false locational signals in order to raise alarm regarding non-existent navigational emergencies (Alcaide and Llave, 2020). The growing concern is that with recent technological advances, cyber-attacks could affect the control of navigational and communication systems such as the AIS used in tracking ships through transceivers, ECDIS, and control systems used to control a ship's ballast, engines and propulsion mechanisms, and cargo management and operation systems (BIMCO, 2021). The safety of these critical maritime systems to support Australian supply chains could thus be compromised.

As reported by the Australian Cyber Security Centre (ACSC) Australian maritime organisations are ill-prepared to withstand cyber-attacks taking place currently (ACSC, 2021). A series of high-profile cyber-attacks in the Australian maritime industry has put cybersecurity in the spotlight (Shipping Australia, 2020). Examples include Austal, an Australian defence contractor, the seaport authority for Geelong Port, and the Toll Group, a giant international shipping and logistics company. These companies have all been recent victims of cyber-attacks with different impacts on their businesses (Chris, 2019, Crozier, 2020a, Crozier, 2020b). Over the years we have seen a number of cyber-attacks aimed at the maritime industry, as highlighted by Table 4.2.

Table 4.2: Recent cyber-attack targets, impact and description

Date	Target	Impact	Description
May, 2021.	Colonial Pipeline	• Network outage. • Fuel shortage. • $4.4 million ransom payment.	Ransomware attack on its computer systems, forcing the company to move some of its systems offline and shut down a major pipeline (Turton and Mehrotra, 2021).
October, 2020.	IMO (International	• Network outage.	Malware attack that disabled their website and intranet, forcing the IMO organisation to shut

	Maritime Organisation)		down key systems to prevent further damage (Konrad, 2020).
September, 2020.	CMA CGM Group	• Network outage. • Data infiltration.	Ransomware attack on its Chinese offices, forcing the container line to shut down network and online services to prevent further damage (Shen and Baker, 2020).
September, 2020.	US tugboat	• Email spoofing.	Phishing attack involving a malware email which spoofed the vessel operator, who then inadvertently sent it on to the vessel via an email attachment (Grasso, 2020).
June, 2020.	Shahid Rajaee Port	• Data infiltration. • Damaged Port system.	Malware attack on an Iranian port on the Strait of Hormuz that crashed the port's computer systems and caused transport chaos for days, attributed to Israel (Al-Jazeera-Media-Network, 2021).
May, 2020.	Toll Group	• Network outage. • Data theft.	Ransomware attack using 'Nefilim' software, which led to stolen personal and business information and caused the shut-down of IT systems to prevent further damage (Reynolds, 2020).
April, 2020.	MSC	• Network outage.	Malware attack that affected systems at the shipping line's Geneva headquarters, resulting in disruption but minimal damage (Twining, 2020).
February, 2020.	Toll Group	• Network outage. • Data theft.	Ransomware attack using 'Netwalker' software that hit land and sea operations. The attackers shut down systems, caused delays and disruptions, attributed to Russian hackers (Reynolds, 2020).
July, 2019.	Stena Impero	• GPS spoofing. • GPS outage. • Navigation disruption. • Ship detained.	GPS spoofing of a UK oil tanker that sent it off course as it entered the Strait of Hormuz where Iran seized ship and its 23 crew, attributed to Iran (Bockmann, 2019).

Source: Kuhn et al. (2021, p. 199) and Turton and Mehrotra (2021)

The purpose of this section is to document different types of cyber security threats to the maritime logistics network in the Indo-Pacific Region. The sectiont describes four key scenarios, which were formulated through an initial project scenario thinking workshop. Under each what-if scenario, the likely impact of cyber threats to the Australian maritime networks was explored using a series of real-world case studies. These case studies may assist in the examination of how such a cyber threat can impact shipping destined to and from Australian ports and the impact upon Australia's maritime supply chain.

4.2. Cyber Security Threat Scenarios

In this section, the what-if cyber security scenarios (also referred to below as "suppositions"), are supported by real life examples. The use of the scenarios has enabled the impact and response to various cyber situations impacting Australian maritime logistics networks to be investigated. These scenarios were developed based upon an earlier project scenario workshop, which ascertained impact and uncertainty scales of cyber security threats to Australian maritime logistics networks. These scales were used to develop four key what-if scenarios. Under the high-impact and high-certainty situations, the disruption to navigational capabilities (scenarios 1 and 2) and physical cyber-physical infrastructure disruption (scenario 3) were identified. These high impact cyber security events are relatively well known, yet they are neither sufficiently documented nor scrutinised to inform strategic actions and policies in Australia in relation to maritime systems. The other scenarios used in the workshop were based upon the cyber-attacks causing disruption on maritime supply chains disruption (imports) (scenario 4) and maritime supply chains disruption (exports) (scenario 5). These scenario descriptions are represented in Figure 4.1.

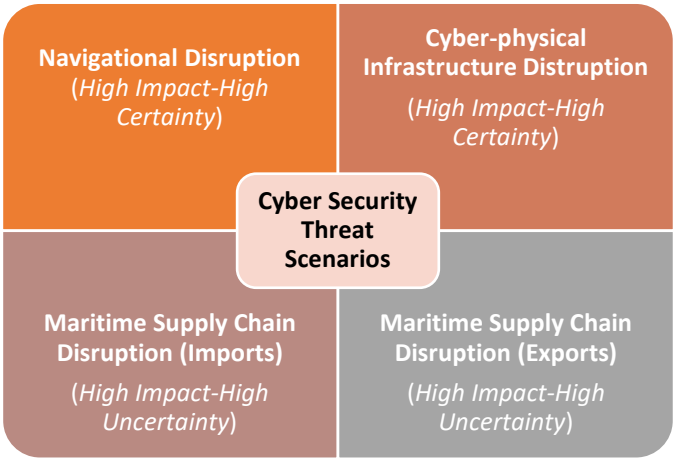


Figure 4.1: Scenario Descriptions

4.2.1. Navigational disruption

Background

The navigation disruption scenario reflects cyber security threat situations where the capacity and capabilities of navigation-critical systems such as the AIS, ECDIS, and the global navigation satellite system (GNSS), are reduced or lost. Other key systems such as the container tracking system, and Port Management Information Systems, or Port Call, are equally at risk of failure or cyber-attack (IMO, 2022). Given the rapid pace of port automation and self-directed vessel navigation, cyber-attacks on system vulnerabilities are likely to become more common place. This means that cyber-attacks will severely affect navigation capabilities of shipping lines and other logistics support systems. For example, autonomous and remote-controlled ships that are currently being developed may become more vulnerable to cyber-attacks (IMO, 2022). Cyber-enabled ships are highly vulnerable to cyber-attacks as they are either autonomous or remotely controlled. These interconnected cyber-physical systems perform certain key onboard ship navigation and communications functions and can be the target of cyber attacks.

Vessels rely on the GNSS to obtain fast, accurate and real-time information to navigate, measure speed, and determine location and plan routes. GNSS is comprised of a number of separate international satellite systems including GPS (US), GLONASS (Russia), Baidu (China) and Galileo (EU) (Korolov, 2019). Disruption of any one of these systems raises fundamental security and safety

concerns. Jamming where the reception of broadcast communications is interfered with, or spoofing, where the perpetrator(s) pretend to be someone else to win trust, can be accomplished with cheap, commercially-available and portable software-defined radio. This is a radio communication system, running open-source software, which typically costs less than US$300. GNSS jamming results in signals being disrupted. However, GNSS spoofing is particularly dangerous as false signals are more difficult to detect (Korolov, 2019).

In the maritime industry, there have been several incidents where GNSS signals to the receivers have been jammed or blocked (see next section). In GNSS jamming, hackers broadcast their interference signals in the GNSS frequency bands (for example GPS L1 - 1575.42 MHz and GLONASS L1OF - 1602.0 MHz). GNSS receivers are then unable to accurately determine position and location (INTERTANKO, 2019). With GNSS spoofing, signal attackers are able to broadcast false GNSS signals or rebroadcast genuine signals captured elsewhere or at a different time. False GNSS signals enable the broadcast of fake signals which are initially synchronised with the genuine signals, and then are gradually replaced using a re-transmitted device (INTERTANKO, 2019). GNSS spoofing has affected ships' electronic navigation capabilities, leading to ships veering off course, becoming grounded, or colliding with other vessels (Shapiro et al., 2018).

There are a number of real examples where GNSS interferences have been observed along coastlines including seaports. These incidents have been largely attributed to interferences to signals from unknown state actors. The examples are:

i. The Stena Impreo case in 2019. The UK oil tanker Stena Impreo strayed unknowingly into Iranian controlled waters. It was later determined that the GPS signal to the ship had been spoofed in the Strait of Hormuz and the Persian Gulf. Subsequently the ship and its crew were detained by Iranian authorities (Bockmann, 2019).

ii. The Black Sea case in 2017. in the commercial seaport of Novorossiysk, Russia. This was the first documented case of GPS spoofing (Scientist, 2017). On 22 June, the captain of a ship off the Russian port of Novorossiysk discovered their GPS had put him in the wrong spot, more than 32 kilometres inland, at Gelendzhik Airport. After checking the navigation equipment was working properly, the captain contacted other nearby ships. It was found that least, 20 ships had been impacted by the same problem.

iii. The North Korean – South Korean border case in 2011, 2012 (World, 2012) and 2016 (Reuters, 2016). In 2016 it was found that GPS signal jamming along the North -South border coastline of the Korean Peninsula, affected thousands of aircraft and fishing ships. In another case, in March 2011, GPS jamming signals from North Korea lasted for 10 days during an annual U.S-South Korea joint military drill. In 2012, a week of GPS jamming affected 337 commercial flights and 122 ships (including a passenger liner and a petroleum tanker) (World, 2012).

iv. The Helge Instad Sola TS case. In this case, in November 2018, the Norwegian warship HNoMS Helge Ingstad (Fridtjof Nansen class frigate) collided with the Maltese oil tanker, the Sola TS (Auer, 2018). This event came after a series of GPS jamming incidents during a NATO military exercise several hundred miles from Norway's border with Russia (BBC, 2018).

v. Persistent GPS outages in the Suez Canal hasve plagued the Egyptian shipping industry since 2017 (Dunn, 2020). Some initial assessments suggested that ‘Ever Given’ ship incident in Suez Canal in March 2021 could have been linked to a weather situation (BBC, 2021) but now the cause is considered technical (including cyber) or human related. Lloyd's List estimated the stranded ship held of nearly US$9.6 billion per day of trade along the waterway.

vi. The Wakashio case in August 2020 (Degnarain, 2020). In this case, the Wakashio oil tanker had been off course for four days sailing through the Indian Ocean, before it crashed into Mauritius' Coral Reefs at a cruising speed, splitting the ship in two parts, causing oil spills across the coast of Mauritius Leading up to the event, investigators had already identified an anomaly within the Wakashio ship's ECDIS (Degnarain, 2020).

There are number of consequences of these types of attacks, these include:

i. Economic – (Rizos, 2021) identified the economic losses according to cyber attacks on navigational systems to commercial shipping. For example, in terms of a cyber incident in the Malacca Straits the strait runs between Malaysia and Indonesia any incident here would have the potential to stop all east–west traffic between the Pacific and Indian Oceans through the South China Sea. In terms of Australia, we would see an economic contraction of between 1.9% and 3.1% (Rizos, 2021);

ii. Navigational - Key consequences of shipping navigation systems being compromised are that ships may veer off course leading to physical detention (as was the case in the Stena Impero case), or collision (the Helge Ingstad case);

iii. Environmental - the environmental consequences caused by the sinking of a ship due to disruption to navigational systems as in the Wakashio incident.

Suppositions (cyber security scenarios supported by real-life examples)

Supposition 1: Attacks on Australian destined shipping in the Malacca Straits.

Over seven days, shipping in the Malacca Straits has been impacted through GPS jamming from an unknown attacker. GPS navigation systems on board the 1,400 ships (including Australian bound ships) that travel through the Straits during the week (Qu and Meng, 2012) have disrupted their AIS (Automatic identification systems) tracking systems. Therefore, traditional manual navigation methods including triangulation and resection, dead-reckoning, and astronomical observations have been resorted to. This has necessitated reduced travelling speeds, and inherent spatial uncertainty due in part to the methods being used and the potential of human error. This has resulted in shipping lanes becoming clogged and several near misses have taken place. As ships have now been delayed, this has resulted in key supply chains throughout the region, being disrupted. Oil supply from the Middle East has resulted in Australia having less than three months of strategic oil reserves.

Supposition 2: Attacks on Australian Bound shipping in the Lombok Strait.

The Lombok Strait provides a key shipping route connecting the Indian Ocean to the Makassar Strait and East Asia via the Sulawesi Sea. It is an important route for Australian north-south bound shipping where 420 ships per year sail the Lombok and Makassar passageway carrying a total of 36 million tonnes of cargo worth US$40 billion (Rusil, 2012).

In this scenario, the Lombok Strait has been impacted for twenty-one days when two autonomous ships in the Lombok Strait have been hacked. This has resulted in the vessels being taken control of and maliciously causing collisions with two other ships in the area. The incident itself and the concern of ongoing hacking incidents meant that the strait was non-operational for twenty-one days.

The incident put a strain on Australian supply chains and caused shortages of key stocks in critical industries, including fuel and certain food stuffs in Australia. In response to the situation and fuel shortages the Australian Government had to implement fuel rationing across Australia. This had a major impact on society, e.g. the impact on food supply chain systems, the impact on medical supply chain systems.

4.2.2. Cyber-Physical infrastructure disruption: Ransomware attacks

Background

The number of ransomware attacks on shipping companies is rapidly increasing around the world (Sadek, 2021). Ransomware is a specific type of malware that freezes IT systems and encrypts data. This can result in authorised access to an organisation's data files becoming blocked and access to data only restored once a ransom (usually in crypto currency) has been paid. With ransomware attacks, the targeted organisation's devices, networks, websites and computer-based platforms are infiltrated, and all its data can become encrypted on drives. This can affect both virtual and hardware-based systems and will render the company's logistics IT systems and communication network systems completely inaccessible. Depending on the extent of the infiltration, the ramifications of the attack could be exceedingly devastating, as reflected in the range and extent of damages caused by recent ransomware attacks on shipping and infrastructure companies around the world (see Table 3).

According to BlueVoyant, a cybersecurity services company, ransomware is the largest cybersecurity threat facing supply chain and logistics companies today (BlueVoyant, 2021). Between 2019 and 2020, the number of ransomware attacks on shipping firms tripled (BlueVoyant, 2021). Citing Israeli cybersecurity specialist Naval Dome, Booth (2021) reports that attempted cyber attacks on the global shipping industry soared by 400% between February and June 2020, due to an increased reliance of the maritime industry on online platforms during the pandemic. Since 2017, the world's four largest shipping companies — Maersk, Mediterranean Shipping Company (MSC), Compagnie Maritime d'Affrètement and Compagnie Générale Maritime (CMA CGM), and China Ocean Shipping Company (COSCO), have all been attacked by ransomware (see details in Table 4.3).

Table 4.3: Examples of Ransomware Attack Cases

Case	**Nature of Attack**	**Extent of Disruptions**	**Estimated Damages**	**Source**
Transnet, July 2021.	Transnet, a South African state-owned rail, port and pipeline company, was attacked using ransomware.	The attack disrupted normal processes and damaged equipment and information, resulting in the company declaring a *force majeure* and halting operations at its container terminals in Durban (handling 60% of South Africa's trade), Ngqura, Port Elizabeth and Cape Town for almost a week before some could resume partial operations. The stoppage resulted in long lines of trucks waiting outside the terminals for hours to	The attack posted a ransom note on Transnet SOC Ltd.'s computers, claiming they encrypted the company's files, and instructing the firm to visit a chat portal on the dark web to enter negotiations.	Booth (2021); Shead (2021); Smith (2021); Wille (2021)

		load and offload their cargo. Most of Transnet's websites remained offline for 11 days until the situation was resolved.		
CMA CGM Group, September, 2020.	French shipping group CMA CGM was attacked by cyber criminals using the Ragnar Locker ransomware.	Services run by the CMA CGM group at a number of Chinese offices, including Shanghai, Shenzhen and Guangzhou, had been disrupted. CMA CGM's group website, including its two subsidiaries, ANL and CNC, became unavailable.	The hackers contacted the company within two days via live chat and demanded payment for the special decryption key. The actual ransom price was not disclosed.	Lloyds List (2020)
Mediterranean Shipping Company (MSC), April 2020.	A ransomware attack from an unknown source caused a network outage at one of the company's data centres in Geneva.	This incident disrupted MSC's official website (msc.com) and its myMSC customer and vendor portal, making them inaccessible to employees, clients, and customers. Some physical computer systems in Geneva were compromised, and some employee and customer data were stolen.	Not disclosed. MSC stated that the attack was confined to a limited number of physical computer systems.	Kovacs (2020)
COSCO (China Ocean Shipping Company), 2018.	Source of the attack was not disclosed. All that COSCO stated about the attack was "Due to local network breakdown within our America regions, local email and	The attack crippled the US network of COSCO, a Chinese shipping conglomerate, locking down its America regions' website and email systems. The malicious code also spread to COSCO's systems in other countries, including Argentina, Brazil,	Not disclosed.	Paganini (2018)

	network telephone cannot work properly at the moment".	Canada, Chile, Panama, Peru, Uruguay, UK and Turkey.		
Maersk, June, 2017.	'NotPetya' was introduced into Maersk's computer-based applications and servers across 600 sites in 130 countries.	Nearly 50,000 endpoints, such as Maersk servers and laptops, were badly infected, including Maersk's laptops sporadically restarting, banks of desktop screens shutdown, physical access gates locked, and corporate phones stopped working.	The attack cost Maersk an estimated US$300 million in lost revenue, information technology restoration, and operational costs.	Palmer (2019); Sadek (2021)

Most ransomware attacks are perpetrated by criminal gangs or rogue state actors seeking financial gain. Unless the demand of the attackers is met, usually in a "ransom" payment made in the form of cryptocurrency, end users within the targeted organisation will either be locked out of their data files or risk being having the stolen data compromised or tampered with (Wille, 2021). Refusal to pay the ransom would mean having to endure months of public relations management and diverting resources to work with the law enforcement agency to investigate and resolve the situation (Wille, 2021). Should a ransomware attack on an Australian Maritime Shipping organisation occur, the malware can spread to many other maritime networks and systems by scanning the entire local system as well as other file systems via the company's intranet. File read-write permissions can become encrypted or overwritten. Vessels in close physical proximity to ports and harbours, once connected with the targeted company's server or network, may also become infected via ransomware.

Supposition (ransomware scenario supported by real-life example)

Supposition 3: Attacks on Australian bound shipping due to ransomware cyber breaches.

Assuming an Australian shipping company were the target of a major ransomware attack on its servers across Europe and India, this could result in ICT system breakdown. This would impact all of the company's business units including container shipping, port operations and tugboat operations, oil and gas production, drilling services, and oil tanker operations. The ransomware attack would disrupt the company's maritime operations in India, Asia and Australia. This would then take the company several weeks to restore its operational capabilities and several months to restore all systems and services to the status before the ransomware attack. This would have a flow-on effect in global supply chains as ships will then arrive late, causing issues in some key export and import supply chains in Australia.

The shipping company would also suffer significant financial losses resulting from the restoration of its ICT systems (re: Maersk case) and customers shifting to competitors during the period of operations disruption and system recovery. While the company may have had all its files backed-up in the cloud, it may succumb to paying the ransom price to avoid having its data files containing customers' records

being tampered with or released on the dark net for use by scammers. The public relations fallout would be unthinkable.

4.2.3. Maritime supply chain disruption

The maritime supply chain disruptions scenarios describe a number of cyber-security scenarios that impact maritime supply chains. These scenarios relate to both imports, where the impact of a cyber-attack on a supply chain that is focused on imported goods into Australia; and exports, where the impact of a cyber-attack is on a supply chain that is focused on exported goods from Australia.

These scenarios describe the different types of consequences that could occur in relation to importing and exporting of goods.

4.2.3.1. Maritime Supply Chain Disruption (Imports): Data breach.

Background

One of the most common types of cyber attacks relate to data breaches. These attacks relate to the disclosure of information usually obtained via hacking of systems. A data breach is defined as being "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored or otherwise processed" (ISO, 2015). Most maritime operators have digitised their business models. This means that that they are at risk of cyber incidents including data breaches.

(Lloyds List, 2021) has estimated that currently one ship per day is being hacked. There have been a number of cyber-attacks linked to Australian maritime organisations that have resulted in data breaches. These are described in Table 4.4.

Table 4.4: Examples of Maritime Data Breaches

Case	**Nature of Attack**	**Extent of Disruptions**	**Estimated Damages**	**Source**
Geelong Port, April 18th, 2019.	External Access to port induction system.	External Unauthored access database files relating to port visitor inductions. The information contained Personally Identifiable Information (PII) information that, when used alone or with other relevant data, can identify an individual.	Limited.	Geelong Advertiser (2019)
Unknown Australian Defence Contractor 2017	Complete external access to Australian Defence subcontractor system.	An Australian Department of Defence subcontractor was hacked and 30GB of "commercially sensitive" documents on projects including the Joint Strike Fighter	Theft of classified information.	IT News (2017)

		(JSF) program and the P-8 Poseidon "submarine killer" plane, as well as detailed designs of Australian Navy ships was taken.		
Austal, 2018.	An attacker stole information from Austal and demanded payment for not disclosing information.	Some ship design drawings for distribution to customers/ subcontractors / suppliers as well as some staff email addresses and mobile phone numbers were stolen by a third party. The third party threated to release the information unless Austal made a payment to the third party.	Limited – internal Austal systems identified the breach.	IT News (2020)

Supposition (based on data breach scenario supported by real-life example)

Supposition 4: Maritime Supply Chain Disruption (Import): Data Breach.

The Australian Government is importing, in large numbers, a new experimental COVID-19 drug treatment drug called Dumnonia. A new COVID variant has been identified, COVID-PI; this new variant is more easily transmittable and unfortunately has a higher mortality rate. Researchers have found that Dumnonia is the most effective drug to treat COVID-PI, but this drug is produced in small numbers and produced by a single pharmaceutical company. Before the COVID-PI variant was identified, Australia bought the existing stock of Dumnonia and arranged for it to be shipped from Europe. An Australian shipping company, Avalon, is handing the shipping of the Dumnonia drug from Europe.

Avalon was a victim of a cyber attack on their corporate information systems from an unknown cyber attacker (the assumption was that the group was linked to a state threat actor) and sensitive information relating to the Dumnonia drug shipment and order information was stolen. The cyber attackers contacted Avalon to demand a ransom of $5 million dollars to be paid in crypto currency or else they will release the information. The ransom was not paid and the cyber attackers released the information relating to Dumnonia, this information contained shipping details, quantity of orders but also cost details of the drug order. The drug manufacturer in Europe considered the Avalon data breach as a breach of contract and cancelled the order of Dumnonia with the Australian Government. The impact was that the new drug was not shipped to Australia and when the COVID-PI variant impacted Australia the mortality rate was much higher than had been expected.

A key consideration is that advanced persistent threat groups, acting on behalf of a state threat actor, undertook the data breach which led to unforeseen consequences occurring in Australia because of the data breach, e.g. mortality.

4.2.3.2. Maritime supply chain disruption (exports): Cyber blockade

Background

Maritime supply chains can become targets for extremist environmentalist groups who may move their actions from physical blockades to cyber-blockades. This would have an enormous impact on export supply chains in Australia. Historically there have been a number of physical blockades on ports in Australia. The Port of Newcastle NSW for example, has been blockaded by several environmentalist groups over recent years. Being the largest port for the export of coal, it has been the target of a number of environmentalist protest groups, decrying the use of fossil fuels such as coal, due to its impact on global warming and sea level rise.

In October 2014, the Pacific Climate Warriors action group, a group of Pacific Islanders, joined an environmental protest blockade using canoes placed across the harbour mouth to prevent the bulk carrier Rhine from departing the Port of Newcastle. This led to a delay to the Rhine's passage out of the port for a short period of time. The group were protesting against the export of coal, signalling its impact on sea level rise throughout the Pacific, due to climate change (The Guardian, 2014).

Again, in May 2016, anti-fossil fuel protests took place across the Port of Newcastle harbour mouth, when protesters used kayaks and boats in an attempt to block the entrance to the harbour (The Guardian, 2016). Organisers of the protests, the Break Free from Fossil Fuels group, estimated that more than 1000 people attended protests in Newcastle, where different groups blocked train tracks used to transport coal to the port.

In November 2021, two protesters entered the Port of Newcastle, scaled and then abseiled down machinery used to load and unload coal, effectively shutting down port operations (Daily Mail, 2021).

Whilst these examples illustrate the disruption caused by physical intervention, a similar situation could occur should a cyber attack occur.

Supposition (cyber blockade scenario supported by real-life example)

Supposition 5: Maritime Supply Chain Disruption (Exports): Cyber blockade.

The Port of Newcastle exported $15 billion of produce including coal during 2013. In 2020, more than 2,200 ships berthed at the port. Two coal ships entering the Port of Newcastle have become victims of a cyber-attack; and all the key systems have been compromised, allowing for external control of the ship. The ships are entering the port via the Hunter River and are now remotely controlled by an external group. The two ships are rammed at full speed at Pirate Point and opposite Pirate Point in the Hunter River. The ramming has caused the ships to sink and become semi-submerged at the mouth of the Hunter River, impacting all port operations. The ship loss also included possible loss of life from the ship's crew and environmental damage.

The Port of Newcastle is now closed for months due to the navigational issues caused by the semi-submerged ships. The incident has now been reported globally. This has had a dramatic impact on the amount of coal exports from the Port of Newcastle.

4.3. Implications

This section has highlighted the vulnerabilities the Australian maritime industry faces due to cyber-attacks on its operations. In the event that such cyber attacks take place, a number of scenarios were discussed. These were supported by real-world examples to demonstrate what disruptions

have taken place and how they have affected supply chains to both imported and exported commodities in Australia.

The following recommendations are made to tackle the challenges that are associated with the cyber security scenarios discussed above:

i. Establishing a mature position on cyber-security, including prescribed back-ups, ransomware policy, and cyber insurance;

ii. Adopting international cybersecurity standards and guidelines such as the US National Institute of Standards and Technology Cyber Security Framework, or ISO 270000, Baltic and International Maritime Council's Guidelines on Cyber Security Onboard Ships, and Australian Cyber Security Standards, such as the Australian Information Security Manuel, ASD Essential Eight;

iii. Improving corporate traditional information systems security and ensuring that security features are tested;

iv. Strengthening the current incident reporting systems and documentation processes to help archive cyber incidents and their impacts;

v. Adopting smart receivers that can operate across multiple GNSS constellations, such as GLONASS, Galileo and BeiDou, or using alternative navigation systems such as Enhanced Long-range Navigation (eLoran) or Galileo's paid Commercial Authentication Service (CAS) to alleviate potential threats;

vi. Incorporating Navigation Message Authentication (NMA), which involves a signal consisting of parts that cannot be generated by a spoofer, into the existing shipboard systems;

vii. Re-aligning the Australian maritime logistics networks to relatively safer and protected countries with critical infrastructure to facilitate urgent re-routing options of essential and critical supplies;

viii. Diversifying supply sources of critical supply chains to mitigate risks associated supply disruption due to maritime conflicts;

ix. Formulating strategic alliances and partnership with countries playing a critical role in Australia-bound shipping to detect potential cyber-attacks early and issue alert of cyber-related disruptions;

x. Exploring possibilities of onshoring and nearshoring to locations outside the zone of potential conflict;

xi. Improving immunity to cyber-attacks and building a cyber resilience culture through raising awareness and staff training in relation to cyber security;

xii. Redesigning jobs of seafarers and shore staff with responsibilities to protect system vulnerabilities, diagnose failures and maintain operative infrastructure from cyber-attacks;

xiii. Better integrating traditional seafarer skills such as traditional navigation methods including triangulation and resection, dead-reckoning, astronomical observations, paper maps, magnetic direction into seafaring training programs;

xiv. The Australian Government's initiatives on maritime cyber security.

5. POLICY ANALYSIS AND RECOMMENDATIONS

5.1. Introduction

This section proposes a security-resilience framework, recapitulates security threats and advances strategies to enhance preparation and prevention, recovery from and adaptation to supply chain disruptions in the Indo-Pacific region. It concludes with a set of recommendations for Australia to address the risks to Indo-Pacific maritime supply chains and their impact on national security and resilience. A security-resilience framework was developed to present the security and resilience aspects and their components and this was used to design a focus group workshop on Indo-Pacific maritime supply chain security for key industry and stakeholder representatives. Using the discussion and feedback from the workshop, maritime security risks and capacity constraints were identified, and policy recommendations for the enhancement of national security and resilience formulated.

The design of the workshop was based on the likely scenarios formulated and the projections made to illustrate the likely outcomes. As discussed in the last section, conflict in the SCS and ECS will force vessels to reroute to avoid the conflict areas. This will extend sailing distance and therefore increase demand for tonnage. In addition, these disruptions, together with increasing risks of cyber attacks, have potential impacts on Australia's national security due to reliance on maritime supply chains for international trade including the import of critical supplies. While Australia relies on a few countries for fuel energy supplies, these countries are directly exposed to maritime security threats in the Indo-Pacific, especially in the SCS and ECS and to any disruption of the larger Indo-Pacific shipping network.

5.2. Security-resilience framework

A security-resilience policy framework was developed and used for the design of an industry and stakeholder focus group workshop, from which the information was collected and analysed to provide policy recommendations. Figure 5.1 presents the key aspects and components of the security-resilience framework. The three main aspects are 'security risks', 'absorptive capacity and resource constraints' and 'resilience'. National resilience has three main components, 'preparedness and prevention', 'recovery', and 'adaptation' (Commonwealth of Australia, 2021, Todorovic et al., 2017).

The framework in Figure 1 also covers the following aspects of national security and resilience:

i. The 'supply chain components' including 'production', 'transport', 'warehousing', and 'distribution'
ii. 'Levels of action' of stakeholders from the organisational, sectoral/industry, and government level.
iii. 'International cooperation' as an important component in the security and resilience of maritime supply chain.

The framework was used to develop discussion questions for the focus group workshop (Appendix 4) and to guide the workshop discussion. It assisted in the collection of participants' comprehensive views on national security and resilience.

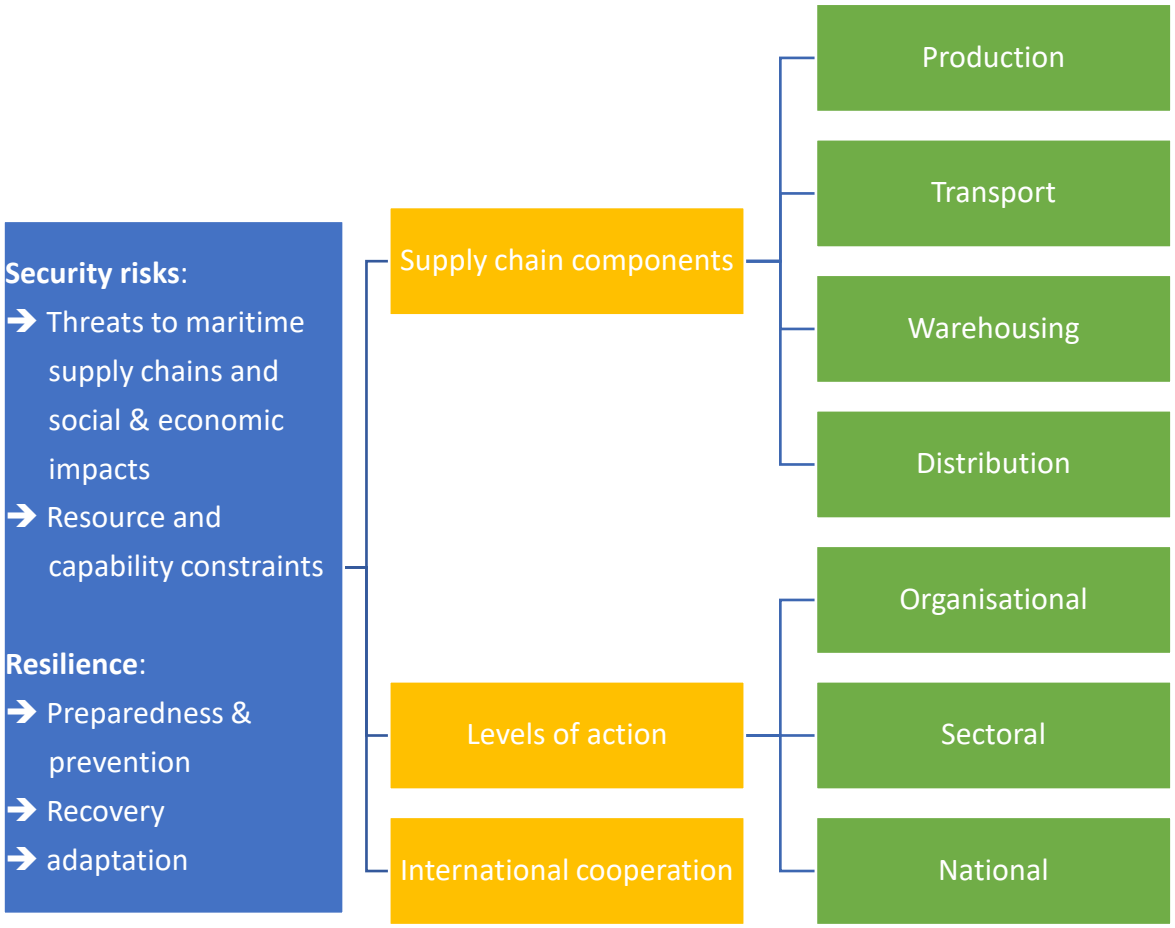


Figure 5.1: Risk-Resilience Policy Framework

Thirty senior-level representatives from maritime transport and logistics related industries, relevant government departments and organisations were invited to participated in the workshop. Sixteen accepted the invitation. Most of the remaining invitees declined due to other commitments. This was in part because, due to COVID-19 restrictions, the workshops were held in early February at a time when many participants were on or returning from leave. Of those that accepted the invitation, thirteen participants took part in the workshop. Together with the nine project team members and a professional workshop facilitator, there were totally twenty-three participants participating in the workshop. Due to research ethical requirement (Research Ethics Approval for project ID 26071), the demographic information of the participants and their respective employers/organisations is not disclosed, and their participation was kept anonymous. The workshop was conducted online via Zoom due to COVID-19 social distancing and travel restrictions.

The workshop commenced with presentations from the project team, where the initial project findings were reported to the workshop participants, providing context for the group discussion. Participants then had an opportunity to ask the project team questions for more detail and clarification. Next, the participants were divided into three groups, each group including a mix of representatives. Group discussion was facilitated by the project team members with the main facilitator providing overall support, moderation and time keeping. Each of the three groups was provided with questions to guide the discussion (see Appendix 4). The discussion points were captured using MURAL, a digital workspace. Each group also provided “the big thing(s)” which highlighted the key point(s} in their discussion.

5.3. Security threats

Figure 5.2 presents a word cloud illustrating an overview of the group discussions on national security. Specific sectors that attracted attention are defence and maritime and logistics sectors. In geographical terms, participants were interested in the Indo-Pacific region and China. Participants have interests in specific issues on security, risk, resilience, capacity, resources, cyber security, connectivity, costs, skills, climate change, and critical supplies (fuel and foods).

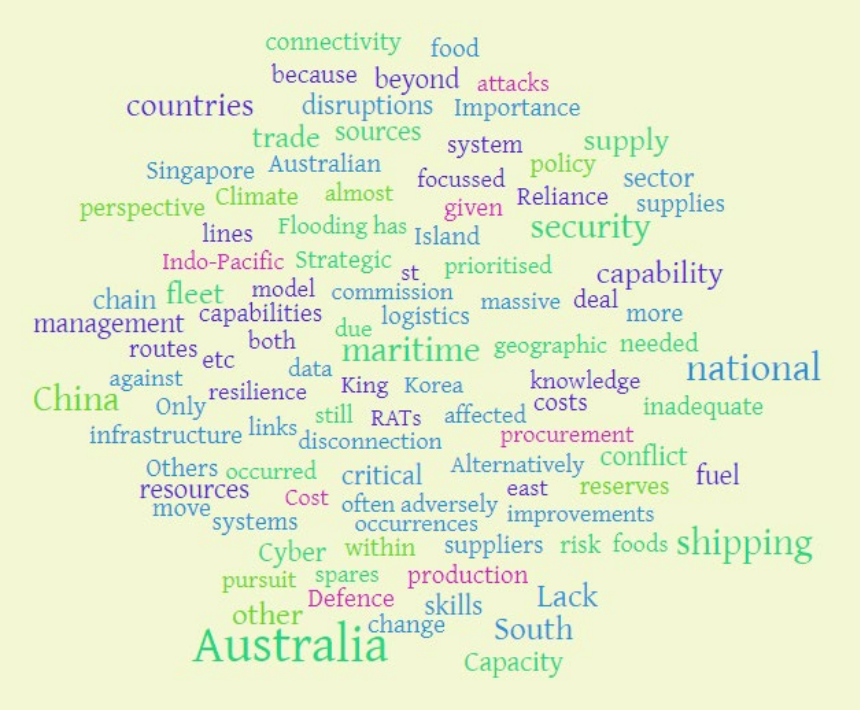


Figure 5 2: National security issues

5.3.1. Security risks

Table 5.1 presents the findings on national security risks from the focus group workshop. Each is supported by statements and phrases expressed by the participants. The first risk is related to reliance for key assets and critical supplies on a few countries including China. The second relates to the dependence on international shipping, lack of a strategic/national fleet and getting data for strategic planning. This leads to the third, the risk of maritime supply chain disruption. It was also considered that “conflict in South China Seas would have a massive impact on trade on Australia” and disruption of Australian maritime supply chains could isolate Australia. Another risk is associated with insufficient maritime infrastructure that is important to the resilience of the maritime logistics system. At the time of writing this report, the Productivity Commission (2022) is conducting an inquiry into Australia's Maritime Logistics System and the report is expected to be released in late May 2022.

The risk to maritime cyber security is increasing as previously noted and “because of web-based port management system being cloud based - not stand alone, and the use of electronic navigation charts”. Vessels and ports targeted by cyber attacks would also cause disruption to the supply chains. In addition, “Climate change threats” were also identified as a risk to national security.

Table 5.1: Security threats and impacts on Australian economic and social security

1. Reliance on a few countries for critical supplies and main exports and imports is a risk to national economy and security
• "Reliance on other countries for key assets"
• "Dependence on China, e.g. Rapid Antigen Tests (RATs)"
• "Vulnerability due to reliance on China"
• "Australia is import focused - export sector, e.g. agriculture sector."
2. Australia relies heavily on international shipping for exports and imports but does not have a national, strategic fleet to ensure continuous operations of maritime supply chains in case of national emergency
• "Importance of controlling shipping to Australia (not necessarily ownership of a national fleet)"
• "Getting access to shipping & supply chain management data for strategic planning"
• "The lack of a strategic fleet is one of the reasons for the failure of Australia's national shipping"
3. Disruption of maritime supply chains could have a potential impact on national security
• "Conflict in South China Seas would have a massive impact on trade on Australia"
• "Broader geographic scale of risk given the globalised trade systems (Suez Canal, Ukraine conflict)"
• "Threat of isolation for Australia"
• "Belt & Road Initiative (BRI) supported by VIC govt and sale of Darwin port to China are examples of lack of security awareness"
4. Maritime infrastructure is insufficient
• "Lack of maritime infrastructure capability"
5. Maritime cyber security risk is increasing
• "Cyber risk because of web-based port management system being cloud based - not stand alone and the use of electronic navigation charts"
• "Ports are subjected to cyber attacks."
6. Climate change is another threat to national security
• "Climate change threats"

5.3.2. Resource and capacity constraints

Resource and capacity constraints are not only a risk to national security but limit the ability to respond to threats and lead to a shortage of imported supplies. Table 5.2 presents the main resource and capacity constraints. The first constraint is insufficient critical reserves for national emergency including "Insufficient stockpiles and fuel reserves", "Lack of capability and resources to deal with emergency and continue production", "Insufficient Australian refining capability". The second constraint concerns the capacity of the logistics system, skills shortages, multimodal and network connectivity across Australian regions, lack of investment and ability to respond to disruption. This limits the national ability to mobilise and respond to national crisis, disasters and disruptions, e.g. pandemics, bushfire and floodings, as experienced recently.

Table 5.2: Resource and capacity constraints in dealing with Indo-Pacific maritime supply chain disruptions

1. Australia has insufficient critical reserves needed in an national emergency
• "Insufficient stockpiles and fuel reserves"

• "Lack of capability and resources to deal with emergency and continue production"
• "Only the basic essentials of vulnerabilities were covered in the productivity commission report but a lot more needed"
• "Fuel rationing scenario with Australia grinding to almost a stall (with only 90 days supply). Insufficient Australian refining capability. South Korea and Singapore sources inadequate"
2. The logistics and supply chain system faces capacity constraints in terms of logistics operations, skills shortages, multimodal and network connectivity across Australian regions, lack of investment and ability to respond to disruption
• "How do we move resources and critical supplies e.g. foods, equipment within the country?"
• "Weakened skills base and loss of production/ manufacturing skills because of pursuit of profit"
• "Australian network connectivity is inadequate"
• "It takes time to build connections within Australia to move food from one part to another"
• "Lack of investment and attention to national domestic connectivity given the size of Australia"
• "Capacities and capabilities to respond to disruptions"
• "Support by trucking or aviation needed for coastal shipping to work"
• "Flooding has affected South Australia and the logistics links between north, south, east and West Australia i.e. nation's logistics systems easily prone to disconnection"
• "Lack of a cohesive national logistics resilience e.g."
• "Free trade agreements with India, etc. do not align with shipping routes that still have to pass through Singapore, Malacca Straights South China Sea"
3. Australia does not have a strategic fleet or sufficient control of shipping service supply to support the nation in emergency
• "Australia does not have control over a national tanker fleet"
• "If conflict occurred - Australia would be dependent on other countries' shipping lines (Example: The UK model of the national fleet)"
• "Lack of maritime capability, knowledge and skills"
• "Maritime not prioritised"
• "Shipping lines are more reactive in their routing and schedules, congestion management, etc. Shipping companies that come to Australia take a commercial perspective (not a defence or national security perspective)"
4. Defence capacity is insufficient to protect Australia maritime trade
• "Defence procurement needs visibility of suppliers and sources of spares and components well beyond 1st, 2nd, 3rd tier suppliers and subcontractors"
• "Triage other elements of national security beyond fuel and food, and beyond China"
• "Australia cannot protect international trade routes"
5. There are issues in Australia's cooperation and relationships with other countries especially in the Indo-Pacific region
• "Security policy improvements and implementation often adversely affect poorer, smaller, weaker countries. Cost of improving security should not be borne by poor neighbours"
• "Pacific Island countries wait for cheaper costs when Australia bids against China. They play both China and Australia to secure best outcomes for themselves e.g. lowest costs, biggest aid funding"

Table 5.2 also suggests the lack of a strategic fleet, control of shipping service supply to support the nation in emergency is another constraint. For example, the lack of a national tanker fleet would limit the capacity to maintain fuel supplies for the economy and respond to disruption of the fuel import

supply chains that are exposed to maritime security threats in the Indo-Pacific discussed earlier. Also related to this constraint is the "Lack of maritime capability, knowledge and skills".

Defence capacity constraints was also identified, including the ability to protect the security of Australian maritime trade in the vast Indo-Pacific, and "visibility of suppliers and sources of spares and components well beyond 1st, 2nd, 3rd tier suppliers and subcontractors." National security also requires the consideration of "elements of national security beyond fuel and food, and beyond China".

The fifth constraint concerns international cooperation and relations with other countries especially those in the Indo-Pacific region. Australia's support to smaller and less-developed countries in the region is important to the strengthening of national security. The rivalry and influence of other countries should also be taken into consideration in international relations. For example, Australia-Solomon Islands relations are subject to not only the unique positions of the two countries but also their relations with and involvement of other countries (Hooton, 2022).

5.4. Implications for resilience strategies

Figure 5.3 presents the key words expressing the views of workshop participants on how to manage and respond to the security risks identified in the last section. Not surprisingly, the term 'Government' was frequently mentioned and the words referring to actors, e.g. 'industry', 'sectors', 'defence', 'maritime', 'freight', 'manufacturing' and 'stakeholders' were also cited.

The policy issues were captured by the terms 'fuel', 'need', 'supply', 'disruption', 'risk', 'threats', 'emergency' and 'China'. Expressions on the geographical extent, 'maritime'/'shipping'/'port', 'national', 'countries', 'regional', 'international'/'global' are aligned to the Indo-Pacific focus of the project.

Words that refer to social economic factors are 'supply'/'supplies', 'demand', 'trade'/'exports'/'imports', 'need'/'needs', 'capacity', 'ownership'. Many terms used to describe policy actions were cited including 'resilience', 'diversification', 'management', 'support', 'monitoring', 'response', 'involvement', 'planning', 'investment', 'develop', 'collaboration', 'diversification'/ 'diversify', 'mitigation', 'prioritise' and 'avoid'.

The next subsections present the findings on national resilience strategies covered in three main areas, preparedness and prevention, recovery, and adaptation.

Figure 5.3: Resilience Strategies

5.4.1. Preparedness and prevention strategies

Preparation and prevention are critical to national resilience, and should be should be aimed primarily at addressing and mitigating security risks. Australia should not only 'expect the unexpected' but also be prepared to deal with it. A scenario planning exercise as discussed earlier is one approach. That is, to identify and evaluate the possible events from which a preparation and prevention plan can be developed. During the workshop, the participants had an opportunity to review the project's initial study results on scenario planning, maritime supply chain security and cyber security. They then discussed how to identify other security risks and develop national resilience strategies accordingly.

Table 5.3 presents seven strategies recommended for Australia's preparedness and prevention of disruption to the maritime supply chains and critical supplies. The first strategy addresses the immediate risk of critical supplies shortages and includes measures such as having sufficient "national reserve of fuel", "diversify the sources of supply and export markets for critical goods including those for new technologies, e.g. rare earth", "develop new manufacturing capabilities", "enhance ability to stockpile", and "broadening security beyond food, fuel and cyber to also include neighbours".

The second strategy seeks to mitigate risks to maritime supply chains. This can be assisted by various mitigation measures such as rerouting to avoid the conflict and congestion areas, monitoring foreign investments in Australian ports, better managing risks to maritime infrastructure, and developing "national Maritime Cyber Security standards".

The third strategy focuses on Australia's international relations. This includes enhancing relationships with neighbour countries in the region, especially, "Australia must engage through the region and consider a similar approach also used by opponents". When managing risk to Australia, the regional context should be taken into account. In addition, "regional neighbours must be strongly befriended especially with regard to logistics, shipping from defence perspective."

Table 5.3: Policy implications for preparedness and prevention

1. Diversify supply sources and avoid heavy reliance on one or few country
• "National reserve of fuel" • "New approach needed as some current approaches do not work e.g. fuel reserves in the US" • "Diversify the sources of supply and export markets for critical goods including those for new technologies, e.g. rare earth" • "Supply source diversification" • "Alternative renewable energy" • "Diversify markets to reduce heavy dependence on a few countries e.g. rock lobster export to China" • "Develop new manufacturing capabilities, e.g. wind farms - needs government support" • "Free trade agreements with non-China trading partners" • "Free trade agreement with EU working on regional trade agreement context" • "Diversification to enhance ability to stockpile" • "Prioritise key issues, e.g. LPG fuel requirements" • "Define and broaden critical products range, to include other areas relevant to defence, not just Productivity Commission's definition and not just essential goods" • "Broadening security beyond food, fuel and cyber to also include neighbours"
2. Mitigate risks to maritime supply chains
• "Route diversification to mitigate disruption risks" • "Foreign investments in dual use ports need to be monitored" • "Explore alternative routeing to avoid South China Sea" • "Mitigate political-economic threats and risks" • "Strategic mapping/rerouting to avoid congestion in freight movements" • "Integrated infrastructure risk (i.e. ports need to be integrated to landside part)" • "Need for national Maritime Cyber Security standards (based on CI standards - minimal standards)"
3. Extend and improve international relations with countries in the region
• "Have arrangements with neighbours forward bases/prepositioning in friendly countries in the region" • "Australia must engage through the region and consider a similar approach also used by opponents" • "Risks need to be identified across the region not just Australia" • "Involvement and risk mitigation of regional conflicts" • "Regional neighbours must be strongly befriended especially with regard to logistics, shipping from defence perspective" • "Utilise Commonwealth platform to enhance seafaring and shipping business"
4. Capacity expansion and infrastructure development
• "More investment in fuel & refining infrastructure in Australia" • "Invest in fuel infrastructure at home and beyond South Korea and Singapore" • "Strategic Australian fleet" • "Increased ownership/ interest in global shipping" • "More seafarers including potential for the immigration program to exert more commercial influence on global shipping" • "Diversify port infrastructure" • "Investment by Australian Government in commercial shipping"

• "Australia should build up and boost its manufacturing industry" • "Australian government subsidise manufacturing, e.g. RATs" • "Maritime be incorporated into national infrastructure planning" • "Australia needs to develop its own capabilities for emergency but the proposed 20 emergency fleet is not enough" • "Land planning and development of infrastructure for freight corridors and freight movements in capital cities/urban areas"
5. Expand defence capacity
• "Strategic fleet for augmentation of Defence effort to support maritime security" • "We must not focus only on the warfare and defence elements but also on shifting trade patterns and build alliances with friendly countries" • "Better urban planning needed for critical infrastructure like ports and warehouses that incorporates a strategic defence and national resilience"
6. A better industrial relations and public-private partnership are needed
• "Public-private partnership needed in contingency planning e.g. fuel supply" • "More balance between public and private sectors needed" • "Cabotage laws need to be reviewed and reconsidered to support building the Australian national fleets (although there may not need to be explicitly fag the ships as Australian to avoid exposing the feet to threats)" • "Reform industrial relations to revitalise Australian shipping" • "Stakeholders' involvement and engagement not happening but needed" • "Linking up also with private organisations for prepositioning in the region" • "History demonstrates a high risk of Government ownership of shipping" • "Ability to adjust to different market situations - organisational agility"
7. Improve Government planning and management
• "Better disruption preparedness and recovery required" • "An integration and participatory approach is needed" • "Government building resilience - needs planning" • "Integration into common funds"

The fourth strategy is to address capacity and resource constraints identified in the previous section. This includes "investment in fuel and refining infrastructure", investment in maritime and logistics infrastructure including "freight corridors and freight movements in capital cities/urban areas", more ownership/control of a "strategic Australian fleet", and build up and boost the manufacturing industry.

The fifth strategy focuses on defence capacity development to support maritime supply chain security, including "augmentation of Defence effort to support maritime security" and the need to incorporate "strategic defence and national resilience".

The sixth strategy entails the improvement of Australia's industrial relations. This can be supported by better public-private partnership, review of cabotage laws, industrial relation reforms to revitalise the Australian shipping sector, and more proactive engagement stakeholders.

The seventh strategy involves improvement of Government planning and management, e.g. using an integration and participatory approach and better planning for Government building resilience.

5.4.2. Recovery strategies

Recovery strategies need to be contingent, continuously monitored and adjusted based on the specific situation and conditions. Table 5.4 presents six general national recovery strategies. The first suggests that Government action and intervention are necessary. In many cases, special and national task forces are needed to provide sufficient support to the situation. Quick and efficient recovery also requires close coordination and collaboration between Government departments.

The second strategy focuses on the efficiency of the use of resources and capacity in the recovery stage. This includes the need to prioritise the needs, “use the "LEAN" approach to emergency response”, and “explore other sources” in order to “overcome limited capacity and resources”. It is also recommended to “use Just in Case (JIC) instead of Just in Time (JIT) against supply chain disruptions”.

The third strategy focuses on the role of public-private partnership in recovery. This includes engagement with the private sector and shipping lines. This should also be supported by the sixth preparedness/prevention strategy mentioned above. Similarly, the fourth strategy aims at ensuring the continuous operation of maritime supply chains and critical supplies, and this strategy should be supported by the second preparedness/prevention strategy to mitigate risks to maritime supply chains.

The fifth strategy addresses the need to continuously monitor the situation and the effectiveness of recovery measures - “monitor the performance and resilience of different sectors and international trade”. The monitoring should cover various levels and segments of the supply chains, in production, warehousing, transport and distribution, as shown in the security-resilience framework. The sixth recovery strategy concerns international cooperation. This strategy should be complemented by the third preparedness and prevention strategy mentioned above.

Table 5.4: Policy implications for recovery

1. Government must intervene
• “Government intervention is necessary.” • “Establishment of government task forces to deal in emergency” • “National response taskforce, similar to the existing for oil spill” • “Collaboration across government departments”
2. Efficient management of resources and capacity
• “Use the "LEAN" approach to emergency response to overcome limited capacity and resources.” • “Explore other sources.” • “Use Just in Case (JIC) instead of Just in Time (JIT) against supply chain disruptions.” • “We must prioritise where the most urgent needs will be proactively when there are disruptions. We are currently too reactive.”
3. Public-private partnership
• “US military gets fuel in Darwin via special arrangement with private organisations.” • “Government needs to engage with shipping lines.” • “Stakeholders’ involvement and engagement not happening but needed”
4. Ensure continuous operation of maritime supply chains and critical supplies
• “Put extra vessels on the routes.”
5. Monitoring the recovery
• “Monitor the performance and resilience of different sectors and international trade”

• "What are the levels/tiers/echelons of supply chain network preparedness we need to address? These need mapping."
6. International collaboration
• "International collaboration with QUAD partners" • "International cooperation (agreements) could provide support in emergency"

5.4.3. Adaptation strategies

Adaptation strategies aim at adjustment to the new situation. Unlike the recovery stage, the adaptation stage is less time sensitive. An adaptation strategy can be carried out in the short or long term depending on its needs. In many ways, adaptation strategies aim to prepare and prevent future disruptions, and therefore are also similar to preparedness/prevention strategies mentioned in Section 5.4.1. Table 5.5 presents three main adaptation strategies. The first focuses on measures that help the economy and society adapt to the new normal, i.e. shortages and disruption of supplies. This includes "develop regional trading hubs" to reduce the reliance on one or few countries. As shown in the previous study on maritime supply chain security, in the case of the closure of and conflict in the SCS and ECS, Singapore remains the fuel supply source least affected. Therefore, "Singapore's critical role to Australia's resilience of international maritime supply chains" should be given more attention. The use of "alternative fuel better sourced locally" and "diversification" are also necessary during the adaptation to the new normal.

Table 5.5: Policy implications for adaptation

1. Adaptation measures are needed under the new normal
• "Develop regional trading hubs to reduce the risk of reliance on a single country, diversify risk and be able to response and adapt more quickly" • "Promote trade relations with India as a key alternative trade partner" • "Singapore's critical role to Australia's resilience of international maritime supply chains" • "Diversification" • "Regular testing cyber-attacks and quick response" • "Alternative fuel better sourced locally" • "The nature of threat galvanises the public and private sectors to make needed investments and changes"
2. Use alternative supplies and sources
• "Greater self-sufficiency of alternative supplies/fuel" • "Innovation and substitution required from a fuel perspective, the use of biofuels through canola oil is one example that has potential Explosive ordnance, pharmaceuticals, food" • "Use of new/ substitute materials instead of using same old inputs whose source and supply is at risk" • "Diversify inputs and raw materials for production of critical goods"
3. Learn from experience
• "Learn from COVID and improving Australia's resilience" • "COVID-19 highlights vulnerability of supply chain management, which could be forgotten once COVID ends" • "Australia cannot build alliances on its own in a very large region. If not for Covid-19 we would not have focused on these issues" • "No threat means no reaction. The Australian government must galvanise society by carefully communicating the threat"

- "Covid-19 raised awareness of supply chain resilience and the need to fully mobilise the public and private sectors"
- "Philippines failed even after winning a judgement against China at UNCLOS (United Nations Convention on the Law of the Sea)"
- "We must make UNCLOS enforceable in all their judgements"
- "We don't have the option of not trading with China, unlike in USSR cold war"

The second strategy also involves the the use alternative supplies and sources. This focuses on "greater self-sufficiency", "innovation and substitution" as well as the "use of new/substitute materials". It is important to also "diversify inputs and raw materials for production of critical goods". The third adaptation strategy is to learn from the experience in order to be better prepared for future unexpected situations. Lessons from the COVID-19 pandemic can be learnt to improve Australia's resilience. One of these, as pointed out earlier, is to foster cooperation and diversify the supply network in the region. In addressing current and future risks, "the Australian government must galvanise society by carefully communicating the threat". Despite concerns about China, "we don't have the option of not trading with China, unlike in USSR cold war."

5.5. Conclusion

In summary, this chapter developed a security-resilience framework for Australia given the reliance on the Indo-Pacific maritime supply chains for critical supplies, international trade and the national economy. The framework covers two main interrelated parts, namely national security risks and resilience, each covering all supply chains components from production to distribution, and at levels of actions from organisation to national. The framework also emphasises the importance of international cooperation. All these were covered in the design of the stakeholder focus group workshop to review national security risks and develop policy recommendations.

The project identified 11 security issues directly and indirectly related to Australia's maritime supply chains. Reliance on one or few countries for critical supplies and main trade is one of major security issues exposing Australia to not only maritime operation risks but also political risks. The lack of ownership and control of a strategic fleet is another issue that needs to be addressed to improve the continuity of critical supplies. Insufficient stockpiles and fuel reserves also exposes the country to security risks. Australia would face the risk of isolation from allies and partners in the Indo-Pacific in case of maritime territorial conflict. External geopolitical influences on the Indo-Pacific region have also become important to national security, given underlying social, economic, politic changes and differences in the region that would affect Australia's strategic position. Insufficient maritime infrastructure and the management of foreign investment in maritime infrastructure are important to national security. Natural disaster and climate change effects have shown increasing intensity and frequency and are an emerging security challenge facing the nation.

Sixteen (16) policy recommendations were made to address the security issues. One of primary focus was the increasing of stockpiles and critical reserves, and the diversification of supply sources and supply chains to mitigate the risk of reliance on a few sources for critical supplies. Development of reliable domestic production capacity would be a sustainable solution to address external supply chain risks. Various measures are needed to improve the security, connectivity and continuity of the Indo-Pacific maritime network, including Government's better control and development of a strategic fleet and critical maritime infrastructure. It was also recommended that the Government takes the leading role in national resilience through active engagement with the private sector, public-private partnership and the participatory approach. The Government should lead national preparedness and

resilience building by promoting national awareness and consciousness of the security and resilience issues.

Australia should take a more active role in the region through international relations and cooperation. The focus should be not only on the warfare and defence elements but also on shifting trade patterns and building alliances with friendly countries in the region. This must also take into account changes in social, economic and political conditions and increasing influences of other countries on the region.

REFERENCES

ACSC. 2021. *ACSC Annual Cyber Threat Report 2020 - 21* [Online]. ACSC. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21 [Accessed 10 December 2021].

AKIMOTO, K. 2017. A new dimension to Australia–Japan maritime security cooperation. *In:* ALAM, M. B. (ed.) *Indo-Pacific maritime security: challenges and cooperation.* Taylor & Francis.

AL-JAZEERA-MEDIA-NETWORK. 2021. *Israel cyberattack caused total disarray at Iran port* [Online]. Available: https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report [Accessed 10 December 2021].

ALCAIDE, J. I. & LLAVE, R. G. 2020. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia,* 45**,** 547-554.

ASIAN, S., CHOI, T.-M. & OLORUNTOBA, R. 2020. Supply Chain Management in an Era of Reglobalization. *International Journal of Physical Distribution & Logistics Management*.

AUER, S. 2018. *Norway warship Helge Ingstad 'warned' before collision. British Broadcasting Corporation* [Online]. Available: https://www.bbc.com/news/world-europe-46150048 [Accessed 10 December 2021].

AUSTRALIAN NAVAL INSTITUTE & NAVAL STUDIES GROUP 2020. *Protecting Australian Maritime Trade,* https://navalinstitute.com.au/wp-content/uploads/Protecting-Australian-Maritime-Trade-Report-March-2020.pdf.

BBC. 2018. *Russia suspected of jamming GPS signal in Finland* [Online]. British Broadcasting Corporation. Available: https://www.bbc.com/news/world-europe-46178940 [Accessed 10 December 2021].

BBC 2020. South China Sea dispute: China's pursuit of resources 'unlawful', says US. 14 July 2020.

BBC. 2021. *The cost of the Suez Canal blockage* [Online]. British Broadcasting Corporation. Available: https://www.bbc.com/news/business-56559073 [Accessed 10 December 2021].

BEECH, H. 2016. Just Where Exactly Did China Get the South China Sea Nine-Dash Line From? *Time,* July 19**,** https://time.com/4412191/nine-dash-line-9-south-china-sea/.

BIMCO. 2021. *The Guidelines on Cyber Security Onboard Ships* [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships [Accessed 10 December 2021].

BLUEVOYANT. 2021. *Supply Chain Disruptions and Cyber Security in the Logistics Industry* [Online]. Available: https://www.bluevoyant.com/resources/gated-resource/cyber-security-and-attacks-in-logistics/ [Accessed 10 December 2021].

BOCKMANN, M. W. 2019. *Seized UK tanker likely 'spoofed' by Iran* [Online]. Available: https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran [Accessed 20 December 2021].

BOCKMANN, M. W. 2022. MR tanker period charters gain 35% in three months. *Lloyd's List,* 23 May.

BOOTH, I. 2021. *Transnet cyberattack could have catastrophic consequences* [Online]. Investec. Available: https://www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html [Accessed 10 December 2021].

BP 2021. *Statistical Review of World Energy 2021*.

BUSZYNSKI, L. 2012. The South China Sea: oil, maritime claims, and US–China strategic rivalry. *The Washington Quarterly,* 35**,** 139-156.

CENTER FOR PREVENTIVE ACTION 2022. Territorial Disputes in the South China Sea. May 04**,** https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.

CHRIS. 2019. *Geelong Port cyber attacked. Infrastructure Magazine* [Online]. Available: https://infrastructuremagazine.com.au/2019/06/19/geelongport-cyber-attacked/ [Accessed 10 December 2021].

COMMONWEALTH OF AUSTRALIA 2021. *Australian Government Crisis Management Framework*.

CROZIER, R. 2020a. *Shipbuilder Austal was hacked with stolen creds sold on dark web* [Online]. Available: https://www.itnews.com.au/news/shipbuilder-austal-was-hacked-with-stolen-creds-sold-on-dark-web-546165 [Accessed 10 December 2021].

CROZIER, R. 2020b. *Toll Group unveils year-long 'accelerated' cyber resilience program* [Online]. Available: https://www.itnews.com.au/news/toll-group-unveils-year-long-accelerated-cyber-resilience-program-551025 [Accessed 10 December 2021].

DAILY MAIL. 2021. *Two female climate protesters shut down the world's biggest coal port by abseiling off crucial machinery* [Online]. Available: https://www.dailymail.co.uk/news/article-10209875/Two-female-climate-protesters-shut-Port-Newcastle.html [Accessed 10 December 2021].

DAS, U. 2019. *What Is the Indo-Pacific? Tokyo: Tribune Content Agency LLC* [Online]. Available: https://thediplomat.com/2019/07/what-is-the-indo-pacific/ [Accessed 8 Deceber 2021].

DAVIS, M. 2019. Forward defence in depth for Australia. *Australian Strategic Policy Institute: Strategic Insights,* 139**,** 1-19.

DEGNARAIN, N. 2020. *Could Oil Ship Wakashio Been Hacked Before Mauritius Spill?* [Online]. Available: https://www.forbes.com/sites/nishandegnarain/2020/10/26/could-mol-chartered-mauritius-oil-spill-ship-wakashio-have-been-hacked/?sh=15d7fae7fbbc [Accessed 10 December 2021].

DEPARTMENT OF DEFENCE 2016. *2016 Defence White Paper,* https://www.defence.gov.au/sites/default/files/2021-08/2016-Defence-White-Paper.pdf.

DEPARTMENT OF DEFENCE 2020. *2020 Defence Strategic Update,* https://www.defence.gov.au/about/publications/2020-defence-strategic-update.

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE 2020. *Trade and investment at a glance 2020,* https://www.dfat.gov.au/publications/trade-and-investment/trade-and-investment-glance-2020.

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE 2022. *Joint Statement on the Supply Chain Resilience Initiative by Australian, Indian and Japanese Trade Ministers,* https://www.dfat.gov.au/news/media-release/joint-statement-supply-chain-resilience-initiative-australian-indian-and-japanese-trade-ministers-0.

DEPARTMENT OF INDUSTRY, S., ENERGY AND RESOURCES, 2019. *Liquid Fuel Security Review,* Canberra.

DEPARTMENT OF INDUSTRY, S., ENERGY AND RESOURCES, 2021. *Australian Energy Update 2021,* Canberra.

DEPARTMENT OF THE ENVIRONMENT AND ENGERY, A. G. 2019. *Liquid Fuel Security Review - Interim Report*, Commonwealth of Australia.

DI LIETO, G. The Securitization of Indo-Pacific Trade and Its New Geo-Economic Paradigms. New Paradigms in the Global Economy, 2018 Beijing

DOLVEN, B., LAWRENCE, S. V. & O'ROURKE, R. 2021. *South China Sea Disputes: Background and U.S. Policy,* https://sgp.fas.org/crs/row/IF10607.pdf, Congressional Research Service.

DUNN, K. 2020. *Mysterious GPS outages are wracking the shipping industry* [Online]. Available: https://fortune.com/longform/gps-outages-maritime-shipping-industry [Accessed 10 December 2021].

GALLAGHER n.d. The 5 most challenging emerging risks facing the Australian maritime industry. https://info.ajg.com.au/hubfs/Documents/The%205%20most%20challenging%20emerging%20risks%20facing%20the%20maritime%20industry.pdf.

GALLOWAY, A. 2021. What's the Indo-Pacific – and how does the Quad work? *The Sydney Moring Herald,* September 16.

GEELONG ADVERTISER. 2019. *Geelong Port targeted in cyber attack* [Online]. Available: https://www.geelongadvertiser.com.au/news/crime-court/geelong-port-targeted-in-cyber-attack/news-story/d6a852664da2a13ec66de060af8e0f60 [Accessed 10 December 2021].

GOPAL, P. 2017. Maritime Security in the Indo-Pacific: The Role of the US and its Allies. *Maritime Affairs: Journal of the National Maritime Foundation of India,* 13**,** 27-40.

GRASSO, M. 2020. *US Tugboat cyber-attack: the experts respond* [Online]. Available: https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/ [Accessed 10 December 2021].
HE, K. & LI, M. 2020. Understanding the dynamics of the Indo-Pacific: US–China strategic competition, regional actors, and beyond. *International Affairs,* 96**,** 1-7.
HIRST, T. 2014. The world's most important trade route? *World Economic Forum,* 21 May.
HOOTON, P. 2022. Solomons security pact: Sogavare, China, and Australia. *The Interpreter,* 21 April.
IMO. 2017. *Maritime Cyber Risk. Guidelines on Maritime Cyber Risk Management* [Online]. International Maritime Organisation. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf [Accessed 10 December 2021].
IMO. 2022. *Autonomous shipping* [Online]. International Maritime Organisation. Available: https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx [Accessed 10 January 2022].
INTERTANKO. 2019. *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)* [Online]. M. G. S. Media. Available: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf [Accessed 10 December 2021].
ISARD, W. 1954. Location theory and trade theory: short-run analysis. *The Quarterly Journal of Economics***,** 305-320.
ISO. 2015. *Information Technology - Security Techniques - Storage Security ISO/IEEC 27040:2015* [Online]. Available: https://www.iso.org/standard/27040.html [Accessed 24 December 2021].
IT NEWS. 2017. *Hacked Aussie Defence firm lost fighter jet, bomb, ship plans* [Online]. Available: https://www.itnews.com.au/news/hacked-aussie-defence-firm-lost-fighter-jet-bomb-ship-plans-475211 [Accessed 24 December 2021].
IT NEWS. 2020. *Shipbuilder Austal was hacked with stolen creds sold on dark web* [Online]. Available: https://www.itnews.com.au/news/shipbuilder-austal-was-hacked-with-stolen-creds-sold-on-dark-web-546165 [Accessed 24 December 2021].
JAIN, S. 2021. *China–Australia relations: Cold politics over hot economics,* https://www.orfonline.org/expert-speak/china-australia-relations-cold-politics-over-hot-economics/.
KANRAK, M., DU, Y. & NGUYEN, H.-O. 2019. Maritime Transport Network Analysis: A Critical Review of Analytical Methods and Applications. *Journal of International Logistics and Trade,* 17**,** 113-122.
KARAHALIOS, H. 2020. Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. *Journal of Transportation Security,* 13**,** 179-201.
KARAMPERIDIS, S., KAPALIDIS, C. & WATSON, T. 2021. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *Journal of Marine Science and Engineering,* 9**,** 1323.
KHURANA, G. 2004. Malacca Strait Security: Is an Extra-Littoral Naval Response Exigent? *Indian Defence Review,* 19**,** 21.
KONRAD, J. 2020. *IMO Cyber-attack has serious implications* [Online]. Available: https://gcaptain.com/imo-cyberattack-has-serious-implications/ [Accessed 10 December 2021].
KOROLOV, M. 2019. *What is GPS spoofing? And how you can defend against it* [Online]. CSO Australia. Available: https://www.csoonline.com/article/3393462/what-is-gps-spoofing-and-how-you-can-defend-against-it.html [Accessed 10 December 2021].
KOVACS, E. 2020. *Shipping Giant MSC Confirms Outage Caused by Malware Attack* [Online]. Available: https://www.securityweek.com/shipping-giant-msc-confirms-outage-caused-malware-attack [Accessed 10 December 2021].

KUHN, K., BICAKCI, S. & SHAIKH, S. A. 2021. COVID-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs,* 20**,** 193-214.
LAGOUVARDOU, S. 2018. Maritime Cyber Security: concepts, problems and models. *Kongens Lyngby, Copenhagen*.
LI, Y. 2019. Economic Development and Evolution of Geo-economic Pattern of the "Indo-Pacific" Region. *Annual Report on the Development of the Indian Ocean Region (2018).* Springer.
LLOYDS LIST. 2020. *CMA CGM confirms ransomware attack* [Online]. Available: https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack [Accessed 11 December 2021].
LLOYDS LIST. 2021. *One ship is hacked every day on average* [Online]. Available: https://lloydslist.maritimeintelligence.informa.com/LL1137457/One-ship-is-hacked-every-day-on-average [Accessed 11 December 2021].
LOWY INSTITUTE 2021. *Asia Power Index Key Findings 2021,* Sydney.
MAHMOUD, M., LIU, Y., HARTMANN, H., STEWART, S., WAGENER, T., SEMMENS, D., STEWART, R., GUPTA, H., DOMINGUEZ, D. & DOMINGUEZ, F. 2009. A formal framework for scenario development in support of environmental decision-making. *Environmental Modelling & Software,* 24**,** 798-808.
MAKINDA, S. M. 1998. Sovereignty and global security. *Security Dialogue,* 29**,** 281-292.
MEDCALF, R. 2018. Reimagining Asia: From Asia-Pacific to Indo-Pacific. *International Relations and Asia's Southern Tier.* Springer.
MEDCALF, R., HEINRICHS, R. & JONES, J. 2011. *Crisis and Confidence: Major Powers and Maritime Security in Indo-Pacific Asia,* Double Bay, NSW, Lowy Institute for International Policy.
MEG KEEN 2021. The China-Solomons security deal has been signed – time to move on from megaphone diplomacy. *The Guardian,* 30 April https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy.
MOCHIZUKI, M. & HAN, J. 2020. Is China Escalating Tensions With Japan in the East China Sea? *The Diplomat,* 19 September.
NICAISE, V. 2021. *Cybermarétique: a short history of cyberattacks against ports* [Online]. Available: https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/ [Accessed 10 December 2021].
OLIVEIRA, A. C. G. D. 2021. From panda to dragon: An analysis of China's maritime actions and reactions in the East China Sea and their implications since 2012. *Contexto Internacional,* 43**,** 147-171.
PAGANINI, P. 2018. *Ransomware attack against COSCO spread beyond its US network to Americas* [Online]. Security Affairs. Available: https://securityaffairs.co/wordpress/74941/malware/cosco-ransomware-attack-followup.html [Accessed 14 December 2021].
PALMER, D. 2019. *Ransomware: The key lesson Maersk learned from battling the NotPetya attack* [Online]. Available: www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/ [Accessed 10 December 2021].
PANDA, A. 2014. Obama: Senkakus Covered Under US-Japan Security Treaty. *The Diplomat,* 24 April.
PRICE, N. 2021. On the Situation in the South China Sea. *Press Statement.* https://www.state.gov/on-the-situation-in-the-south-china-sea/: U.S. Department of State.
PRODUCTIVITY COMMISSION 2021. Vulnerable supply chains: Productivity Commission study report.
PRODUCTIVITY COMMISSION 2022. *Australia's Maritime Logistics System,* https://www.pc.gov.au/inquiries/current/maritime-logistics#draft.
QU, X. & MENG, Q. 2012. The economic importance of the Straits of Malacca and Singapore: An extreme-scenario analysis. *Transportation Research Part E: Logistics and Transportation Review,* 48**,** 258-265.

REUTERS. 2016. *South Korea revives GPS backup project after blaming North for jamming* [Online]. Available: https://www.reuters.com/article/us-shipping-southkorea-navigation/south-korea-revives-gps-backup-project-after-blaming-north-for-jamming-idUSKCN0XT01T [Accessed 10 December 2021].

REYNOLDS, Z. 2020. *Toll Logistics hit by second cyber attack* [Online]. Available: https://safetyatsea.net/news/2020/cyber-crimes-land-second-hit-on-toll-logistics/ [Accessed 20 December 2021].

RIZOS, C. 2021. *GNSS 'in Troubled Waters* [Online]. Tac Talks. Available: https://www.navy.gov.au/sites/default/files/documents/Tac_Talks_Issue_10_2021.pdf [Accessed 10 December 2021].

ROSALES, J. J. 2019. The South China Sea: A Strategic Flashpoint. ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS FORT LEAVENWORTH ….

ROYAL AUSTRALIAN NAVY 2010. *Australian Maritime Doctrine,* https://www.navy.gov.au/sites/default/files/documents/Amd2010.pdf.

ROYAL AUSTRALIAN NAVY 2017. *Australian Maritime Operations,* https://www.navy.gov.au/sites/default/files/documents/Australian_Maritime_Operations_2017.pdf.

RUSIL, M. 2012. *Maritime Highways of Southeast Asia: Alternative Straits?* [Online]. Available: https://www.rsis.edu.sg/rsis-publication/rsis/1686-maritime-highways-of-southeast/#.YfKLF_lByUl [Accessed 18 December 2021].

SADEK, N. 2021. *Shipping Companies Confront Cyber Crooks as Economies Reopen. Bloomberg Government* [Online]. Available: https://about.bgov.com/news/shipping-companies-confront-cyber-crooks-as-economies-reopen/ [Accessed 18 December 2021].

SATAKE, T. & SAHASHI, R. 2021. The Rise of China and Japan's 'Vision'for Free and Open Indo-Pacific. *Journal of Contemporary China,* 30**,** 18-35.

SCIENTIST, N. 2017. *Ships fooled in GPS spoofing attack suggest Russian cyberweapon* [Online]. Available: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 12 December 2021].

SENATOR REYNOLDS 2019. *ASPI International Conference: War in 2025,* https://www.minister.defence.gov.au/minister/lreynolds/speeches/aspi-international-conference-war-2025, Australian Department of Defence.

SHAPIRO, L. R., MARAS, M.-H., VELOTTI, L., PICKMAN, S., WEI, H.-L. & TILL, R. 2018. Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security,* 11**,** 65-83.

SHEAD, S. 2021. *South Africa port operations halted and workers reportedly put on leave after major cyberattack* [Online]. CNBC. Available: https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html [Accessed 10 December 2021].

SHEN, C. & BAKER, J. 2020. *CMA CGM confirms ransomware attack* [Online]. Available: https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack [Accessed 10 December 2021].

SHIPPING AUSTRALIA. 2020. *Cyber Security: Preventing the Ghost in the Machine. Shipping Australia Limited* [Online]. Available: https://www.shippingaustralia.com.au/cyber-security-preventing-the-ghost-in-the-machine/ [Accessed 10 December 2021].

SMITH, C. 2021. *Transnet cyberattack: Main ports at 100%, but warehousing and cold storage still impacted* [Online]. Available: https://www.news24.com/fin24/economy/transnet-cyberattack-main-ports-at-100-but-warehousing-and-cold-storage-still-impacted-20210730 [Accessed 10 December 2021].

TAYLOR, B. 2014. The South China Sea is not a flashpoint. *The Washington Quarterly,* 37**,** 99-111.

TERTIA, J. & PERWITA, A. A. B. 2018. Maritime Security in Indo-Pacific: Issues, Challenges, and Prospects. *Jurnal Ilmiah Hubungan Internasional,* 14**,** 77-95.

THE GUARDIAN. 2014. *Pacific Islanders blockade Newcastle coal port to protest rising sea levels* [Online]. Available: https://www.theguardian.com/environment/2014/oct/17/pacific-

islanders-blockade-newcastle-coal-port-to-protest-rising-sea-levels [Accessed 20 December 2021].
THE GUARDIAN. 2016. *Dozens arrested as anti-fossil fuel protesters join Australian coal blockade* [Online]. Available: https://www.theguardian.com/environment/2016/may/08/hundreds-of-anti-fossil-fuel-protesters-join-australian-coal-blockade [Accessed 20 December 2021].
THE GUARDIAN. 2021. *China's hypersonic missile test 'close to Sputnik moment', says US general* [Online]. The Guardian Australian Edition Available: https://www.theguardian.com/us-news/2021/oct/28/chinas-hypersonic-missile-test-close-to-sputnik-moment-says-us-general [Accessed 8 January 2022].
TILLETT, A. & CONNORS, E. 2020. New bloc of Australia, India, Indonesia takes shape amid China fears. *Australian Financial Review*.
TINBERGEN, J. 1962. *Shaping the world economy; suggestions for an international economic policy,* New York, The Twentieth Century Fund.
TODOROVIC, B., TRIFUNOVIC, D., JONEV, K. & FILIPOVIC, M. 2017. Contribution to Enhancement of Critical Infrastructure Resilience in Serbia. *In:* LINKOV, I. & PALMA-OLIVEIRA, J. M. (eds.) *Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security.* Springer.
TURTON, W. & MEHROTRA, K. 2021. *Hackers Breached Colonial Pipeline Using Compromised Password* [Online]. Bloomberg News. Available: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Accessed 20 December 2021].
TWINING, G. 2020. *MSC confirm malware attack* [Online]. Available: https://safetyatsea.net/news/2020/msc-confirm-malwareattack/ [Accessed 20 December 2021].
US DEPARTMENT OF DEFENSE 2019. *Indo-Pacific Strategy Report: Prepareness, Partnership, and Promoting a Networked Region,* https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF.
VILLAR, L. & HAMILTON, M. 2017. *The Strait of Malacca, a key oil trade chokepoint, links the Indian and Pacific Oceans,* https://www.eia.gov/todayinenergy/detail.php?id=32452, U.S. Energy Information Administration.
WANG, A. 2021. Chinese military holds live-fire drills in East China Sea amid Taiwan tension. *South China Morning Post,* 3 Nov.
WHITE, H. 2021. Australia's seaborne trade: Essential but undefendable. *The Interpreter.*
WILLE, M. 2021. *Hacked CD Projekt Red data is floating around the internet* [Online]. INPUT. Available: https://www.inputmag.com/gaming/hacked-cd-projekt-red-data-is-floating-around-the-internet-company-says [Accessed 20 December 2021].
WILLE, M. 2021 *CD Projekt Red hit by ransomware attack, says it won't pay up* [Online]. INPUT Available: https://www.inputmag.com/gaming/cd-projekt-red-hit-by-ransomware-attack-says-it-wont-pay-up [Accessed 10 December 2021].
WORLD, G. 2012. *Massive GPS Jamming Attack by North Korea* [Online]. Available: https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/ [Accessed 10 December 2021].
YILMAZ, S. & LIU, F. K. 2022. Disputes in the South China Sea: Does the Arctic Council offer a viable regional governance model? *Asian Politics & Policy,* 14**,** 7-24.
YOSHIHARA, T. 2013. The US Navy's Indo–Pacific challenge. *Journal of the Indian Ocean Region,* 9**,** 90-103.
ZAHIR, A. 2021. *Militarization, Power Projection, and Territorial Disputes In the South China Sea,* Dhaka, Centre for Governance Studies.
ZHAO, S. 2020. East Asian Disorder: China and the South China Sea Disputes. *Asian Survey,* 60**,** 490-509.

APPENDIX

Appendix 1: Case study: Toll Group

Incident descriptions: Toll Group, which operates in Australia, has been hit twice by cyber-attacks in February and May 2020 (Smith, 2020a, 2020b). The first attack was in February 2020. Attackers locked the company's computer system and encrypted all of its files, causing Toll's network outage, delays, disruptions and data loss. There is evidence that Mailto actors have used phishing and password spray attacks to access accounts and then used these compromised accounts to spread the malware through users' address book. The malware was identified as a relatively new variant of the 'Mailto' ransomware, and the attack used 'Netwalker' software to hit land and sea operations. The attack was attributed to Russian hackers (Kuhn et al., 2021). In May 2020, the latter was conducted. Logistics giant Toll Group had closed internal and customer-facing systems after being infected by a new form of ransomware (Smith, 2020a). The attackers used a new form of ransomware known as 'Nefilim' software, which led to stolen personal and business information and caused the shutdown of most online customer applications (i.e., moving to offline) and other IT systems to prevent further damage (Kuhn et al., 2021).

Response: Toll Group had isolated the problem and was gradually bringing its systems back up online by reinstating back-end hardware and testing key systems internally and with some customers. Toll Group used backups to make restorations of their key online systems. Toll has embarked on an "accelerated cyber resilience program," and security team rebuilds. They worked closely with world-class cyber experts to drive large-scale projects across critical pillars, such as identity and access management, security architecture, security risk management, and many more (Crozier, 2020b).

Appendix 2: Case study: Geelong Port

Incident descriptions: In April 2019, an employee's email account was breached, causing a data breach of its electronically stored information such as visitor induction names and driver licences. This data was available for access by an unauthorised party.

Response: The suspected data breach was then identified, immediately disabled the breached email account and enabled additional security measures. Geelong Port commenced a formal investigation into the cause of the breach and commenced a review of all data in the account. In conjunction with its IT supplier, further steps are being taken to reduce the risk of any future attacks. Geelong Port has notified the Office of the Australia Information Commissioner of the incident (Chris, 2019).

Appendix 3: Case study: Austal

Incident: Austal is the Australia's biggest defence exporter and a major shipbuilder for the US Navy. Austal also builds patrol vessels and frigates for the Australian Navy. In mid-October 2018, an unknown offender from the Middle East had bought some of Austal's staff email passwords from the dark web, then accessed some staff email addresses and mobile phone numbers. The hackers also stole ship design drawings, which were distributed to customers, subcontractors, or suppliers and were neither sensitive nor classified. The criminals threatened to sell Austal's stolen data on the dark web and engaged in extortion.

Response: As the attackers triggered an alarm when they stockpiled data for exfiltration, the Information Systems and Technology (IS&T) team locked the system up, shut down all the external ports, and made sure no information could move in and out. Austal referred the breach and extortion attempt to the Australian Cyber Security Centre (ACSC), federal police and the Department of Defence. Austal also confirmed that there is no evidence to suggest that information affecting national security, nor the company's commercial operations have been stolen. With the assistance of the ACSC, Austal embarked on a "spring clean" of its systems. Austal's system and data were cloud-based and have been backed up. Austal has put in an Australian-developed software tool that forces users to set more complex passwords and to change them frequently. It also used multi-factor authentication and tightened access privileges to a range of internal systems (Crozier, 2020a).

Appendix 4: Focus group workshop discussion questions

	Key aspects and dimensions		
	Supply chain components: production, transport, warehousing & distribution	**Levels of action: organisational, sectoral & national level**	**International cooperation**
Part 1: National risks associated with Indo-Pac maritime supply chains (considering participants' perspective on MSC risks and impacts)			
Question 1: Apart from those presented so far in this project, are there any other threats to Indo-Pacific maritime security? How may they affect Australian economic and social security? Alternatively, how vulnerable overall are Australian maritime supply chains to conflicts, pandemics, climate change, cyber attacks and other security threats in the Indo-Pacific?			
Question 2: Do we have adequate resources (capacity) and capabilities (technical, logistical) to deal with: i) the occurrences (e.g., alternative sources of critical supplies), and ii) the consequences (e.g., the different types of impacts on the national economy) of these disruptions?			

Alternatively, what are the limitations of the current system to cope with the prospective Indo-Pacific maritime supply chain disruptions?			
Part 2: Breakout group discussion on policy implications (domestic & international) on each of the following components of national resilience: • **Preparedness & prevention** • **Recovery** • **Adaptation**			
Question 1: How can Australia be better **<u>prepared</u>** to respond to Indo-Pacific maritime supply chain (MSC) disruptions? Alternatively, how can Australia manage the risks associated with Indo-Pacific MSC disruptions? Note: What has been done well and what not, considering the current policy on e.g. alternative sources of critical supplies, energy reserve, national reserve, domestic production, capacity building, infrastructure development, strategic fleet, international arrangements/initiatives?			

Question 2: How can Australia **recover** from Indo-Pacific maritime supply chain disruptions? Note: Consider policy on vessel re-routing, response taskforce capacity building, strategic fleet, international arrangements/initiatives, etc.			
Question 3: How could Australia better **adapt** to a new normal associated Indo-Pacific maritime supply chain disruptions in the future?			