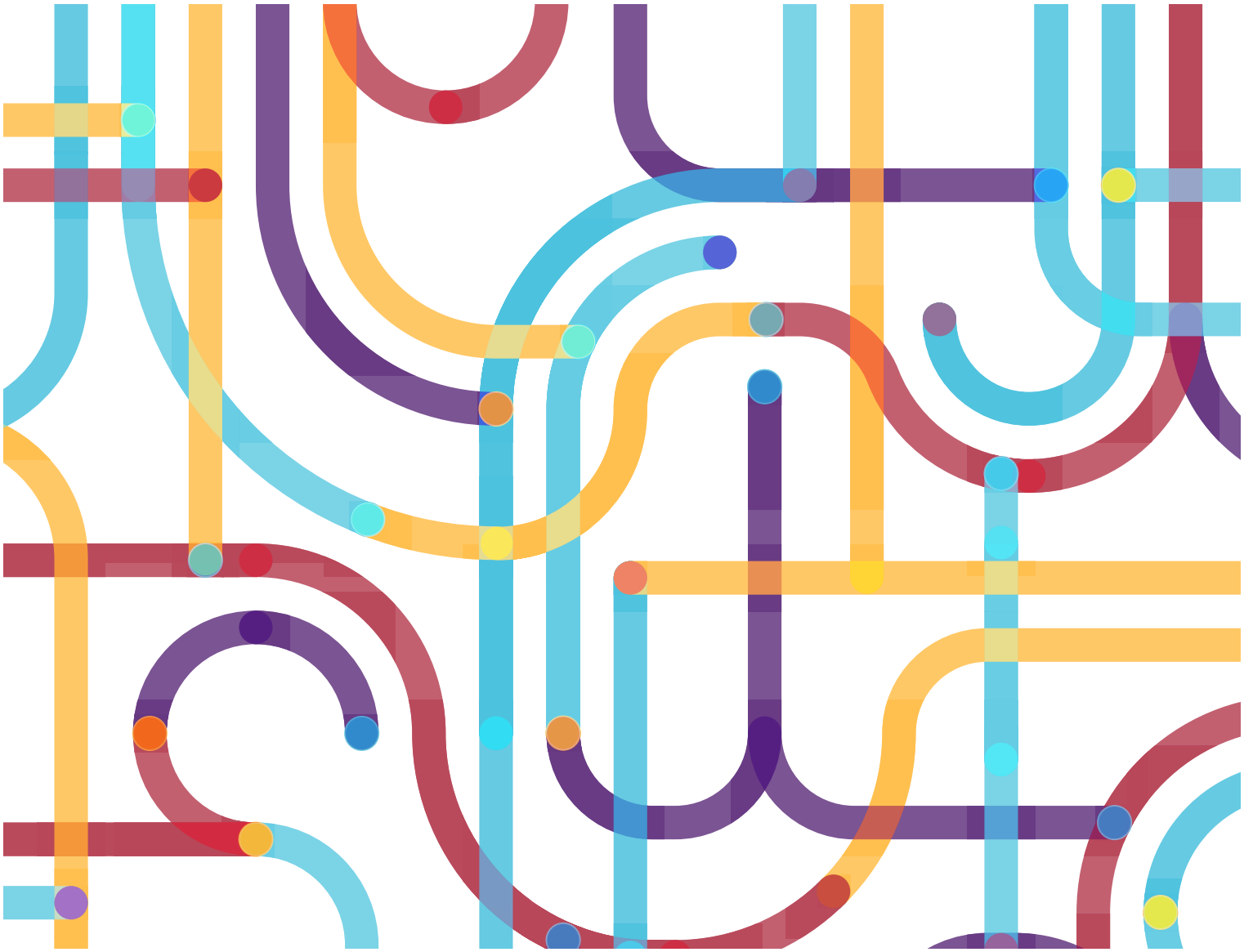
AIGROUP
DEFENCE COUNCIL

Perth USAsia Centre

Securing Australia's Defence Supply Chains

AUGUST 2022



Securing Australia's Defence Supply Chains

AUGUST 2022

AIGROUP DEFENCE COUNCIL

Perth USAsia Centre

Contents

Executive summary

The security of Australia's global supply chains is under increasing strain. This is driven by both 'traditional' supply chain challenges such as the COVID-19 pandemic, as well as 'strategic' factors associated with rising geopolitical competition.

While supply chain risks are felt economy-wide, they are especially pressing for Defence and defence industries. There is now a widely recognised need to invest in improving the resilience of defence supply chains.

Since 2020, a range of new strategies have been developed to improve the security of Australian defence supply chains. Similar efforts have been launched by our allies and defence partners, including the US, UK, Japan and several others.

This report investigates strategies for increasing the resilience of Australia's defence supply chains. Supported by the Department of Defence's *Strategic Policy Grants Program*, the Australian Industry Group and Perth USAsia Centre evaluated current supply chain frameworks and practices in light of traditional, emerging and strategic risks.

Consultations were undertaken with over 60 stakeholders from both Defence and defence industry to generate insights into the nature of contemporary supply chain vulnerabilities and risk management practices.

The report finds that Defence and defence industry have matured their supply chain approach in recent years, including via investments in new tools and capabilities to identify and protect vulnerabilities. However, there remains areas where further effort is required.

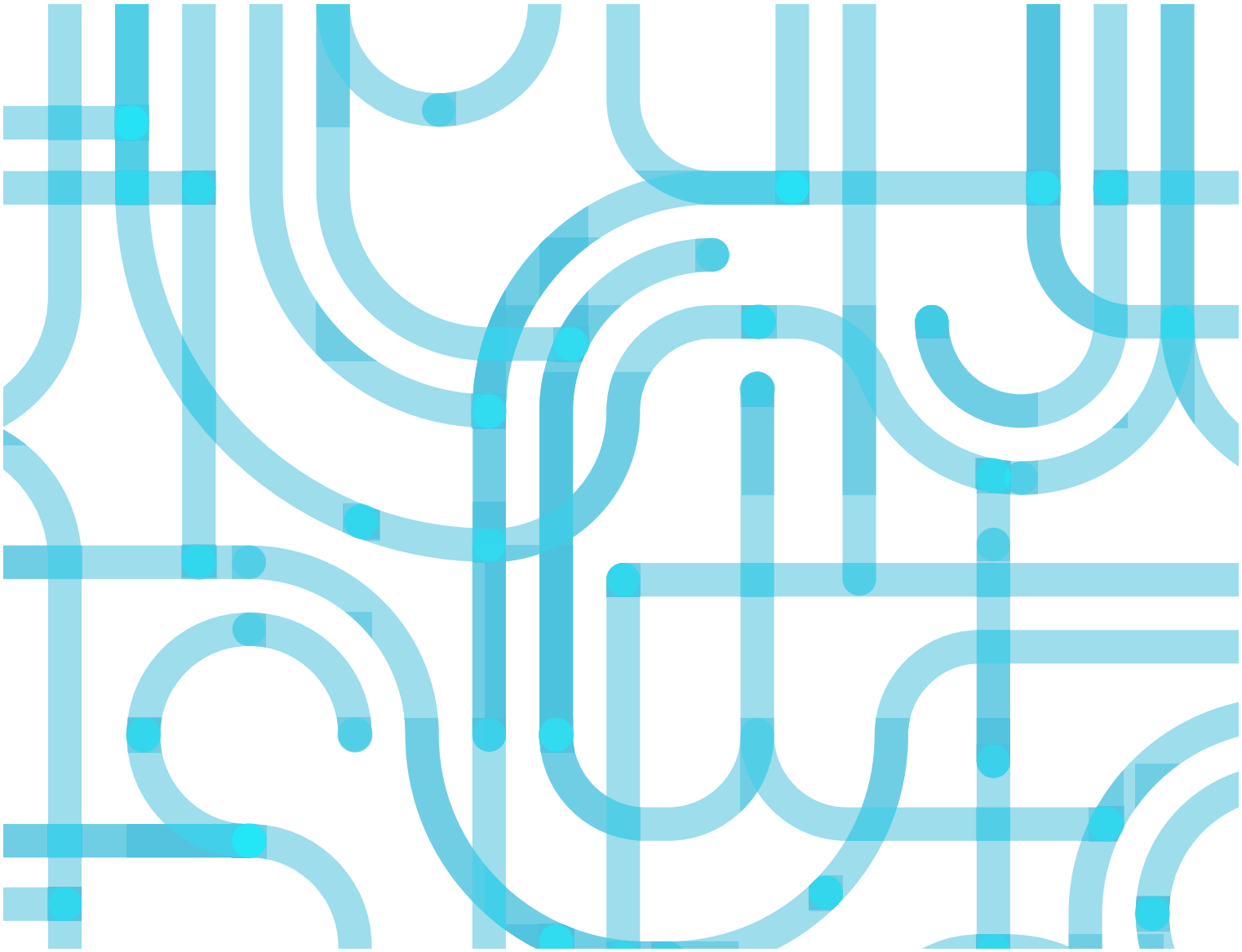
Decision-makers require more detailed information on the structure of defence supply chains, particularly beyond first and second tier suppliers. Limited visibility over the deeper levels of the supply chain obscures mission-critical vulnerabilities that may present during a crisis.

As strategic risks to supply chains increase, stronger governance structures and policy frameworks are also required. These should set core concepts and definitions for supply chain security, provide risk assessment frameworks, and identify options for interventions to address identified vulnerabilities. Undertaking a cost-benefit analysis, examining options and determining the resources required to make supply chains more resilient will be key to success.

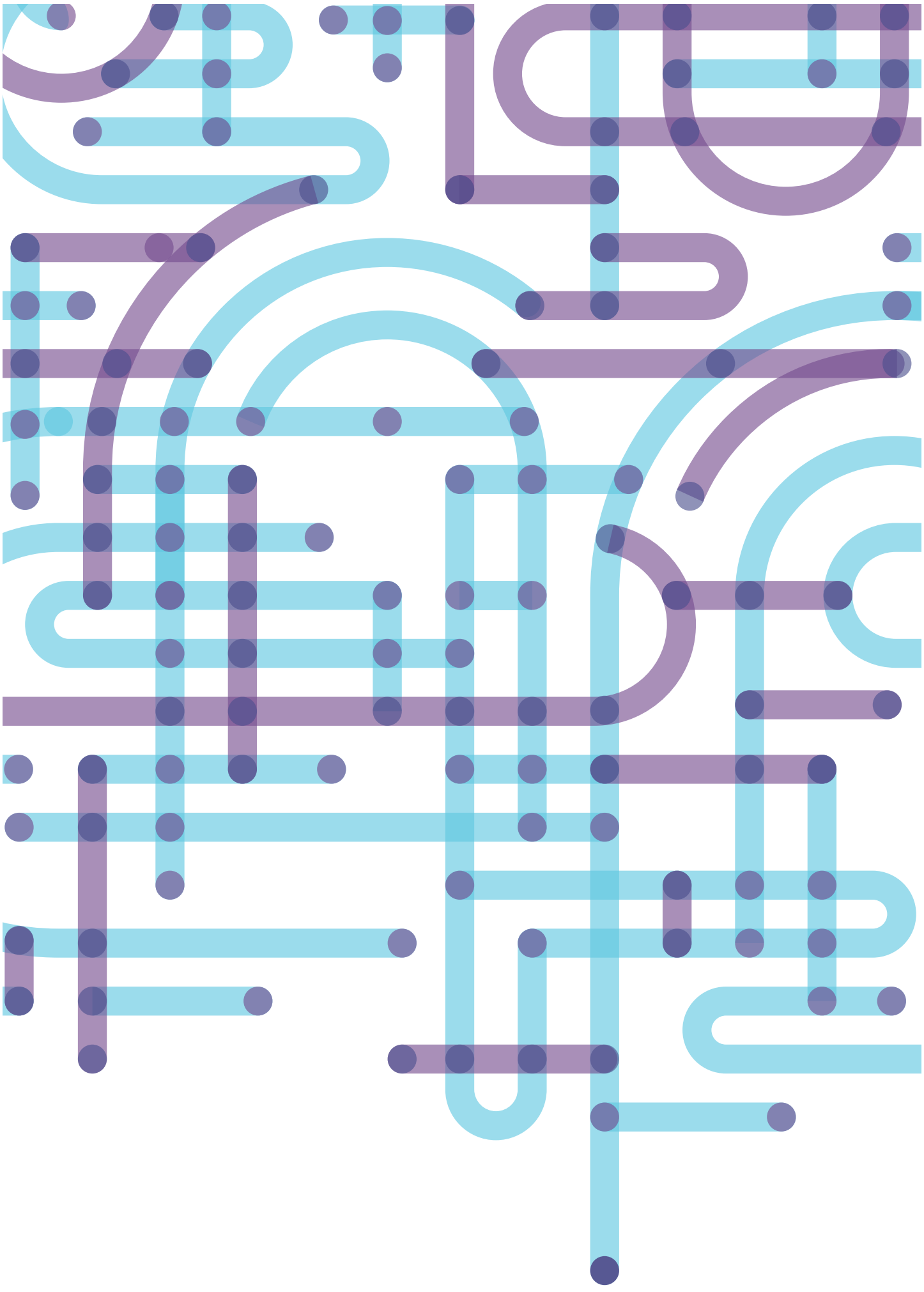
Greater collaboration with defence industry is critical to achieving supply chain security. This can be achieved through information sharing and consultation with industry, as well as a sharper focus on supply chain issues during procurement and contracting.

As Australia's allies and partners undertake similar efforts, there are opportunities for international collaboration for defence supply chain resilience. Both government-to-government and industry-to-industry partnerships offer opportunities for Australia to build 'trusted' defence supply chains with likeminded partners.

Key research findings



- Both 'traditional' and 'strategic' supply chain risks facing Defence and defence industry are rapidly increasing.
- While Defence and defence industry are still focussed on 'traditional' risks, such as logistics and commercial availability, awareness of strategic risks is rising. An example of this growing awareness relates to fuel and fuel reserves.
- Interruptions associated with COVID-19 have exacerbated potential vulnerabilities in the last two years.
- Strategic risks – resulting from politically-induced interruptions – have not yet posed interruptions to defence supply chains. However, Australia's deteriorating geostrategic environment, as set out in the 2020 *Defence Strategic Update*, mean these interruptions may credibly pose such risks in the future.
- Strategic risks are not yet afforded a consistent level of priority between Defence and defence industry.
- Since the 2020 *Defence Strategic Update* and *Force Structure Plan*, a range of new policies and strategies have been developed to augment supply chain resilience. Additional resources have been committed to addressing identified risks.
- Australia's key defence partners are also developing new supply chain security efforts, with similar objectives and approaches. Australian policy and strategy development is approximately on par with the US and UK, and slightly ahead of other regional partners.
- Defence and defence industry have matured their supply chain approaches in recent years. Defence has invested in the use of new tools, including through the use of automated tools such as the Supply Network Analysis Program (SNAP).
- Defence has used these tools to run supply chain risk analyses, and we understand the findings have identified new risks which should be elevated to a strategic priority.
- However detailed information on the structure of defence supply chains – particularly beyond first and second tier suppliers – is not widely available to Defence or defence industry on a comprehensive basis.
- There is a need for a governance structure for regular and organised engagement between Defence and defence industry. This should include both information sharing mechanisms for the identification and reporting of vulnerabilities, and consultation mechanisms for developing mitigation measures.
- There is a need to develop frameworks to inform the design of supply chain security interventions, particularly to ensure that interventions are resource-efficient and proportionate to identified risks.
- The concept of 'industry as a fundamental input to capability' is still maturing in Defence. Further developing it will help underpin supply chain security throughout the capability life cycle.
- Supply chain considerations should be incorporated into the full Defence capability life cycle. Supply chain issues need to be considered at the very start of the project life cycle, and systematically incorporated into project development, acquisition, contracting and sustainment.
- A key question in this context is how to strike the cost-benefit balance for interventions.
- A framework should be developed to identify the thresholds for consideration when designing options and intervention strategies.
- Greater resourcing will be required to manage growing strategic risks to defence supply chains. The quantum and form of resourcing should be determined following new risk assessment exercises.
- There are opportunities to collaborate with allies and international partners as Australia further develops its defence supply chain approaches. The US and UK are ideal partners, in light of the AUKUS agreement and their similar stage in policy development.
- The Australian Government's proposed Defence Industry Development Strategy offers an opportunity to embed supply chain within the Defence context.



Introduction

Australia faces increasing pressures on the global supply chains connecting national industries to the global economy. Risks to supply chains have emerged due to 'natural' events, most prominently the COVID-19 pandemic which has interrupted trade connections across the world. But they have also arisen due to political factors, including increasing geostrategic competition and the use of protectionism and/or coercive trade policies by many governments.

While the effects of these supply chain risks are felt economy-wide, they are especially pressing for defence industries, as well as other defence-adjacent 'critical goods' sectors. The 2020 *Defence Strategic Update* and *Force Structure Plan* both identify supply chain security as a central policy challenge. The *Defence Strategic Update* notes that *"The pandemic has disrupted globalised supply chains, which over time have become a critical element of many of Australia's national economic sectors and Defence capability planning"*[1].

There is now a widely recognised need to invest in improving defence supply chain resilience, particularly efforts to develop 'trusted' trade relationships.

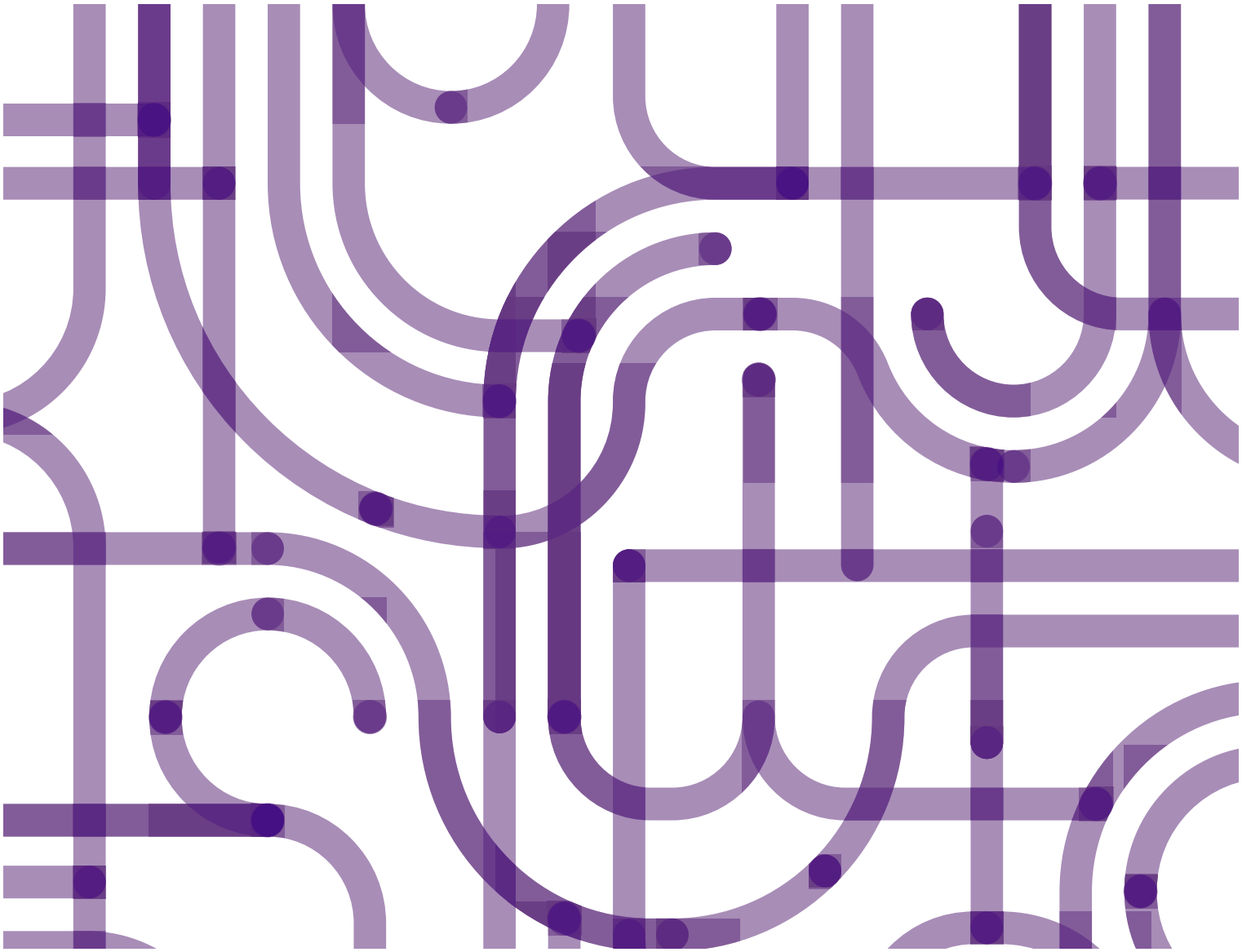
However, improving supply chain resilience is a costly endeavour, and finite resources must be strategically focussed on areas where risks and their impacts are greatest. This requires methods for evaluating defence supply chain risks, so that resilience initiatives can be targeted to maximise effectiveness. Existing supply chain management frameworks are not calibrated to capture the nature of traditional and strategic risks to Australia's external trade relations.

Defence, defence industry and wider government will benefit from an agreed framework to identify these risks, evaluate their impact, and inform the design of targeted supply chain resilience measures.

This report investigates the current state of play in Australia's defence supply chains, and strategies that can be used to address emerging risks. Supported by the Department of Defence's *Strategic Policy Grants Program*, and developed in consultation with policy and industry stakeholders across the Australian defence sector, the report identifies mechanisms Defence and defence industry can deploy to improve the resilience of supply chains in a period of economic and political pressure.

It finds that a clear and contemporary understanding of supply chain risks is still maturing in the Australian defence sector, and that there is a need to augment current practices designed to manage 'traditional' supply chain risks with new measures configured to emerging strategic threats. It develops a set of framework principles that should inform the development of new supply chain resilience measures, and proposes concrete recommendations for how these can be implemented in partnership between Defence and defence industry in the near to medium-term.

2 Supply chains, critical products and the defence sector



Global supply chains – the commercial networks which make final products from raw materials – are an inescapable part of contemporary life. Given the complexity and modern technologies, very few products are made in a single country. Rather, they are produced in highly-globalised supply chains, within which many firms across different countries specialise in certain stages of the production process.

These are critical for the supply of sophisticated modern products, as they unlock economies of scale and specialisation that greatly improves the efficiency of the production process.

Complex global supply chains first emerged in the 1970s, when consumer goods industries such as clothing began outsourcing some stages of production to Asia. In the years since, global supply chains have become a common industrial model across all sectors, but they are especially prominent in high-technology industries which depend on specialised skills and knowledge. As a result, they are now the dominant industrial model for defence industries, given the technological complexity of modern military platforms. Global defence companies – known as "Primes" in Australia[2] – are a significant part of the Defence procurement process. They help to organise and manage a range of defence supply chains on behalf of governments under procurement contracts. Small to medium-sized enterprises (SMEs) have also developed capacity and capability in Australia and have grown their own supply chains.

The label "supply chain" conveys the impression that these networks involve the *supply* of commodities across borders: first as raw materials, then as processed components, and finally as the finished goods supplied to end users. However, this impression is misleading, as the interactions between players in global supply chains are far more complex than simply supplying physical goods. Three distinct but interconnected relationships connect supply chain participants:

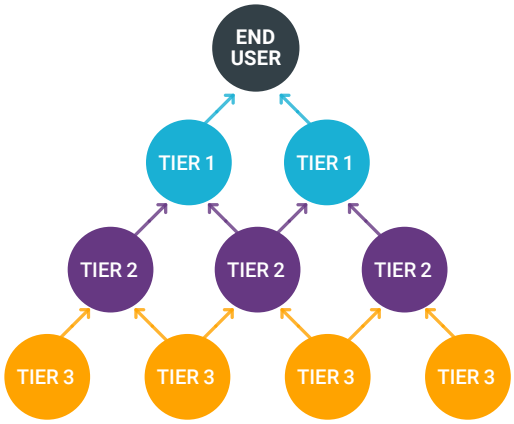
1. **Flows of materials** – the commodities themselves, as they pass through sequential stages of production in different countries.
2. **Flows of capital** – the commercial arrangements between firms within a supply chain, including cross-investments and contracting arrangements to manage their interconnections.
3. **Flows of knowledge** – the intellectual property and services involved in a supply chain, both directly shared between participating firms and/or embodied within goods and people.

These flows create relationships of interdependence that connect the players within a global supply chain. Countries and firms do not only trade goods between each other, but develop long-term and institutionalised commercial relationships that integrate the disparate parts of the system. While a final product will be labelled as "Made In" a particular country and firm, its supply ultimately depends on an interconnected and coordinated global network in which many countries and firms play essential roles. Understanding the structure of these networks is critical to assessing and improving the security of supply of modern products.

Supply chains are also not necessarily a *chain* of relationships. They usually take the form of a web, with multiple participants at each stage of the production process, and overlapping relationships existing between them. Indeed, as Figure 1 illustrates, these webs can also have differing 'geometries', based on the location of critical nodes within the supply chain.

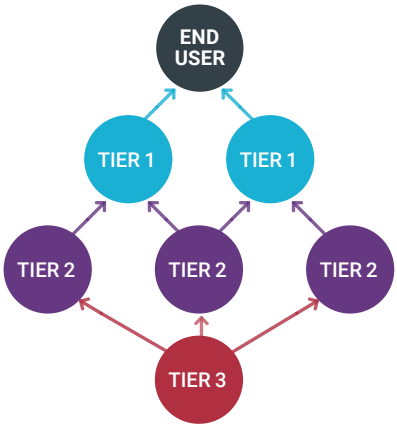
Examples of supply chain geometries

The number and location of 'critical' nodes (**in red**) within a supply chain differs based on its geometry.



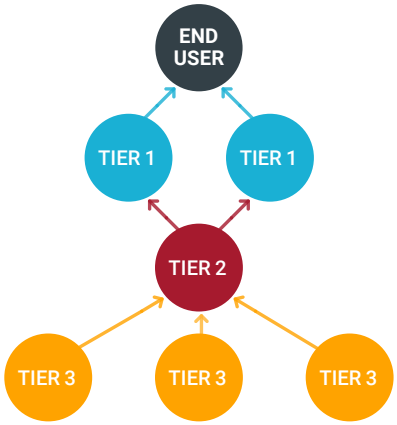
Branching supply chains

Where downstream users source inputs from multiple suppliers, which each have multiple suppliers, flowing back through multiple steps. This is the most competitive and resilient type of supply chain, as there are no critical nodes that are reliant on a single participant.



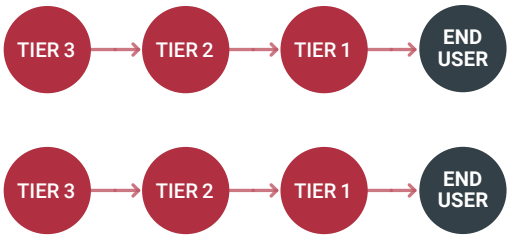
Diamond supply chains

Where downstream users source from multiple suppliers, but those suppliers ultimately all source from a single upstream point of origin. Concentration at the upstream source acts as a critical node, on which all participants further along the chain depend.



Hourglass supply chains

Where there are multiple downstream users and upstream suppliers, but dependence on a single player at the midstream stage. Concentration at the midstream is a critical node on which both ends of the value chain depend.



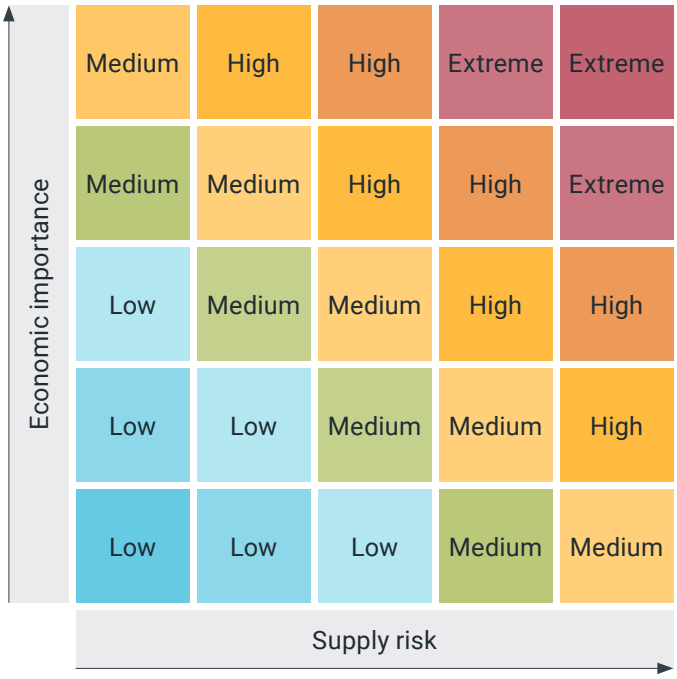
Linear supply chains

*W*here each downstream user maintains its own chain of mid- and upstream suppliers, all of which are critical nodes. These are the least resilient type of supply chain and, as a result, occur only rarely in highly specialised products.

The criticality matrix

The concept of "criticality" is central to distinguishing between different types of global supply chains. Critical goods and services are a special category of economic activities, which are defined by their outsized importance to the supply chains of which they are a part. The commonly used definition[3] of a critical product identifies them as having two distinct features: very high *economic importance* for the industries that rely upon them, face *supply risks* that can interrupt their availability and/or affordability. This two-part definition distinguishes critical products from those which face only one condition, such as foodstuffs (economic importance only) or jewellery (supply risk only). Critical products are only those which satisfy both conditions.

FIGURE 2: THE CRITICALITY MATRIX

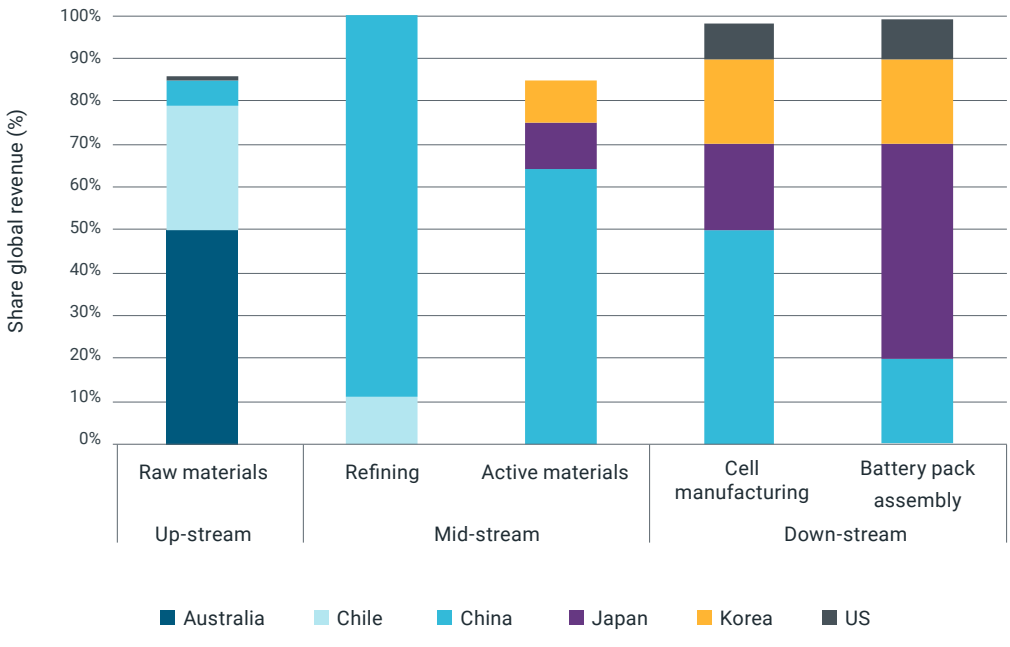


Many factors affect whether a particular product should be classified as critical or not. For economic importance, it includes whether the product is essential to meet end users' needs, and the existence of readily available substitutes with similar or near-similar properties. For supply risk, factors include whether a product is locally produced or imported, the extent to which its supply is subject to monopoly by a small number of producers, and the prospects of political conflicts leading to an interruption of supply. These risk factors are inherently qualitative and can change rapidly over time. They also vary between end users – an input which is essential for one application may not be for another. For this reason, there is no universally-agreed or fixed list of critical products, and criticality must be continuously assessed by each end user.

Criticality is the main variable that determines the resilience of global supply chains. Where the geometry contains one or many critical nodes – the diamond and hourglass supply chains – there is limited capacity to respond to exogenous shocks. By contrast, a supply chain without critical nodes (such as the branching supply chain) has in-built capacity to adjust around shocks. Importantly, the existence of critical nodes is often opaque to non-adjacent participants. In diamond or hourglass supply chains, end users with multiple tier 1 suppliers may be unaware that a critical node exists further back along the chain.

The challenge posed by 'hidden' critical nodes is illustrated by the global value chains for battery production. Contemporary battery value chains have an hourglass structure, where one country – China – dominates the production of midstream components (Figure 3). While there is diversity of suppliers at the upstream (mining) and downstream (battery assembly) stages, participants at both ends depend upon refining and materials processing done in China. Lithium, which is mined in Australia and ultimately used in a Japanese-made battery, nonetheless requires midstream processing in China. As a result, China's market power in the global battery industry is significantly greater than that suggested by its 20 per cent share of final product sales. By assessing the full

FIGURE 3 :
COUNTRY SHARES OF BATTERY VALUE CHAIN BY STAGE OF PRODUCTION



Source: Accenture 2021

length of a global supply chain, critical nodes are revealed which would not be apparent when evaluating from either an upstream or downstream perspective alone.

Defence sector supply chains face especially daunting issues in managing criticality. Defence supply chains tend to have a larger number of critical nodes when compared to their civilian counterparts, because of:

1. **Higher economic importance of products**, due to very high operational requirements for defence platforms and less ability to substitute for 'near-similars'.
2. **More concentration in supply chains,** due to exacting design specifications and compliance costs surrounding security requirements that limit the number of participating firms.
3. **Greater reliance on imported goods and services,** as economies of scale can make full local production of some Defence capabilities in small and medium-sized countries uneconomic.
4. **Deeper levels of intellectual property embodied within products,** which requires long-term services relationships between vendors and customers after equipment is delivered.
5. **Higher risk of geopolitical supply interruptions,** due to the strategically important nature of the defence sector.
6. **Longer supply chains** – often extending back ten or more tiers – due to the high-technology nature of modern defence platforms.

As a consequence, defence industry requires significantly greater attention to supply chain risks than in other sectors of the economy. Defence supply chains are more complex, feature more risk points, and face higher continuity expectations than their civilian equivalents. Supply chain risk management strategies for defence need to go well-beyond standard commercial practices, to ensure these sector-specific risks are properly understood and mitigated.

3 Defining and mitigating supply chain risks in the defence sector

The effective management of supply chain risks in the defence sector requires evaluating the factors that lead to interruptions.

While the mapping of a supply chain's geometry will identify risk points (i.e. find the location of critical nodes), the second step is to evaluate the likelihood that these risk points will pose supply interruptions. There are a range of factors that can lead to interruptions, which can be distinguished into two broad categories: traditional and strategic supply chain risks.

Traditional supply chain risks have long existed and affect all industries relatively equally. They comprise the types of risks that commonly occur in globalised industries, including:

1. **Economic risks**, such as sudden demand or technology shocks that lead to temporary shortages of critical goods and services. The recent global semiconductor shortage – which caused several automakers to reduce output in 2021 and produced a knock-on global shortage of automobiles[4] – is a current example.
2. **Infrastructure and connectivity risks,** such as delays in logistics and customs clearances. The six-day obstruction of the Suez Canal in March 2021[5], ongoing congestion problems at many US ports[6], and COVID-related shutdowns at several Chinese mega-ports[7], are three prominent examples that significantly interrupted global logistics flows.
3. **Natural disaster risks,** such as fires, floods, droughts and diseases that inhibit normal commercial operations. The COVID-19 pandemic is a self-evident example. But natural disasters can even affect high-technology industries. The global semiconductor shortage has been exacerbated by drought in Taiwan[8] and industrial fires in Japan[9] that have reduced output at critical supply chain nodes.
4. **Societal conflict risks,** such as mass protests, civil conflicts and labour disputes. These risks occur frequently in the resource sector, exemplified by oil and uranium supply constraints due to recent civil conflict in Kazakhstan[10]. However labour disputes are very common and affect many industries, such as recent industrial action at Fremantle Ports which threatened supply chain continuity for the Western Australia building industry[11].

This category of risks can be labelled 'traditional' because they are an established fact of life in the global economy. They occur regularly and are a normal business risk for global supply chains. Contemporary supply chain management practices have

been developed to manage these traditional risks, in a way that balances the benefits of mitigation efforts – such as holding larger inventories, or maintaining a broader pool of suppliers – against the costs of these policies. While they certainly affect the defence industry, they are not unique to the sector and affect all global supply chains roughly equally. Importantly, traditional supply chain risks are not deliberate, nefarious or political in nature: they "just happen" and businesses need to deploy strategies to manage them when they occur.

By contrast, strategic supply chain risks are relatively new and have particular relevance for the defence sector. They comprise risks that originate from developments in the strategic environment, including:

1. **Geopolitical intervention risks,** where governments make deliberate interventions into supply chains in order to achieve geopolitical goals. Trade sanctions and embargoes are a common tool, for example China's recent use of trade sanctions during recent diplomatic disputes with several countries including Australia[12]. Commercial sanctions against specific companies – such as US national security bans on several Chinese tech companies – are another example.
2. **Geopolitical demand risks,** where the expectations on supply chains rapidly change as a result of geopolitical developments. This might include requirements to remove certain suppliers from the network, due to deteriorating political relationships that suspend trade. For defence and defence-adjacent industries, it can also include 'surge requirements', where demand rapidly increases at a time of geopolitical conflict.
3. **Security risks to intangible assets,** such as cyber-attacks, intellectual property theft and the compromise of security systems. These risks do not specifically target the material flows of commodities within supply chains, but the information and knowledge interdependencies that connect participants within the supply chain.

Strategic supply chain risks are differentiated from traditional risks by being intentional – and often political – acts. They are deliberately executed by hostile actors, with the specific objective of interrupting supply chain integrity. Strategic supply chain risks affect all industries and are already common in the form of commercial espionage and criminally-motivated cyber-security attacks. However, they are a particularly pronounced risk for defence and defence-adjacent supply chains, as these industries are a primary target for politically-motivated attacks. Strategic supply chain risks are also growing fast in the early 21st century, driven by the increasing digitisation of international trade and intensifying levels of geopolitical competition.

The companies which manage globalised industries deploy supply chain management strategies to mitigate the impacts of these risks on business continuity. While many such strategies exist, they can broadly be classified into two types. One type are efficiency-oriented models, which emphasise speed and cost minimisation to deliver products to market most competitively. Offshoring and 'Just-In-Time' (JIT) supply chain practices are a well-known example. The other are resilience-oriented models, which sacrifice pure efficiency in favour of in-built flexibility to manage risks when they occur. 'Just-In-Case' (JIC) practices – where inventories are held to provide insurance against interruptions – is a typical approach.

Importantly, these supply chain management models are not strict alternatives, but exist on a spectrum that trades off efficiency versus risk mitigation requirements. Companies choose a preferred place on this spectrum based on their particular circumstances and their calculations regarding the likelihood of risks occurring. In highly-competitive industries where interruptions are infrequent and/or impose low costs, efficiency-oriented JIT models are the norm. In industries where risks are more frequent and/or costly, resilience-oriented practices are adopted to provide latency when interruptions occur.

When companies perceive the need to build more risk-resilience into supply chains, there are a range of practices they can deploy to minimise the cost of interruptions. These practices vary in terms of their cost and the degree of risk-mitigation that they afford. In order of increasing cost, they include:

- **Strategic inventories:** Holding a greater level of inventory than required for normal business purposes, that can be used during supply interruptions to maintain continuity (warstock). Inventories are especially useful for frequent but temporary supply chain risks (such as economic shocks or natural disasters), which usually resolve themselves in a matter of weeks or months. They are an attractive solution because they do not require changes to supply chain and only impose the costs of warehousing additional inventory. This technique can have limitations if the shelf life is short and usage rates low, for example, with some types of munitions.
- **Supplier diversification:** Bringing a larger number of downstream suppliers into the network than is commercially necessary, to provide a greater range of potential suppliers in the event of interruptions. Ideally, these suppliers should be based in different countries, to minimise impact from national-level risks. Diversification can be used to remove critical nodes within a supply chain, by bringing additional participants in at concentrated stages.
- **Friend-shoring:** Prioritising the inclusion of 'trusted' partners in the supply chain, who are less likely to pose either traditional or strategic supply risks. This can be done at either the national level (towards more friendly countries) and/or corporate levels (towards more reliable businesses). Friend-shoring is useful when critical nodes cannot feasibly be removed from the supply chain, and therefore reliance on a trusted partner at the critical node is used instead.
- **On-shoring/in-housing:** Where a supply chain node is extremely critical, then do it yourself. This can also be done at the national level (making the product domestically) and/or corporate level (in-house production). This can be a higher cost and resource intensive strategy, and complex in the context of high value Defence capabilities (such as fighter jets).

An example which brings together some of these initiatives in the context of fuel security, includes the previous federal Government's announcement of a strategic oil supply, leveraging off the US strategic oil reserve.

All of the above responses to supply chain risks require a solid 'business case', as they can be costly in comparison to alternatives. In competitive and price-sensitive markets, companies will only deploy them when the likelihood and impact of supply chain risks exceed the costs of mitigation strategies. And even in the less-cost sensitive defence sector, it is commercially unviable to adopt these strategies widely across the industrial ecosystem. Rather, these strategies must be deployed in a limited and selective manner, targeted to the most likely sites for supply chain risk to emerge.

The effective management of supply chain risks is therefore one of targeting interventions. Supply chain managers must identify the risk points in their supply chain, assess the criticality of those risk points, and configure targeted responses from the above options that are aligned and proportionate in cost to the risks being mitigated.

4 New policies and frameworks for Australian defence supply chains

Australian defence policy is attuned to these supply chain risks. In recent years, several new frameworks – including the 2016 *Defence White Paper*, the 2020 *Defence Strategic Update*, and their associated policies – have brought a greater degree of attention and resources to bear on supply chain security issues. Together, they provide the broader regulatory frameworks within which supply chain security efforts are nested.

The 2016 Defence White Paper and associated defence industry policies

The 2016 *Defence White Paper* and *Defence Industry Policy Statement* began this process, by setting a new direction for Australian defence industry policy. The *Defence Industry Policy Statement* moved away from the emphasis on buying defence goods and services 'off the shelf' from international partners, towards the development of a more capable industrial base, supported by reorienting procurement to focus on buying Australian content and capability.

While Australia has focussed on development of local capability, we are still a very significant importer of Defence goods and services, which requires significant reliance on overseas supply chains.

Since 2016, the previous federal Government released a range of defence industry policy papers and initiatives, including:

- The Defence Export Strategy, released in 2018, where the previous federal Government expressed an intent to become a top ten Defence exporter.
- The Defence Industrial Capability Plan, released in 2018, which set out a plan for the industrial base and introduced the concept of Sovereign Industrial Capability Priorities (SICPs).
- The Defence Industry Skilling and STEM Strategy, released in 2019.
- Industry support programs, including the Office of Defence Industry Support and the Defence Innovation Hub.
- A new and enhanced Australian Industry Capability (AIC) contractual framework.

These previous federal Government defence industry policies and programs have had a positive impact on developing the industry and increasing the scope of the Australian defence industrial base. According to the Australian Strategic Policy Institute, these policies have materially increased local spend, and noted that from 2019-20 – 2020-21:

'Defence's local military equipment spend grew by a remarkable 35% to around $3.5 billion. Australian industry isn't just growing in absolute terms: there are also signs that it's growing in relative terms compared to the share of spending going overseas.'[13]

This increased scope, capacity and capability of the Australian defence industrial base makes the task of protecting Australian defence supply chains even more critical. This is particularly important because the number of SMEs entering the supply chain is growing as a result of these policies.

The 2020 Defence Strategic Update and Force Structure Plan

In 2020, the previous federal Government issued updates to the initiatives of the *Defence White Paper*, embodied in the *Defence Strategic Update* (DSU) and *Force Structure Plan (FSP)*. These documents place a strong emphasis on the importance of the protection of our supply chains and noted the urgency of understanding the risks to defence supply chains and developing calibrated risk mitigation measures.

The DSU provided an update to the strategic challenges and directions now facing Australia, including a new strategy for capability investment plans. It explicitly noted the link between our reduced strategic warning time for a major conventional attack against Australia and protecting supply:

'Previous Defence planning has assumed a ten-year strategic warning time for a major conventional attack against Australia. This is no longer an appropriate basis for defence planning. Coercion, competition and grey-zone activities directly or indirectly targeting Australian interests are occurring now. Growing regional military capabilities, and the speed at which they can be deployed, mean Australia can no longer rely on a timely warning ahead of conflict occurring. Reduced warning times mean defence plans can no longer assume Australia will have time to gradually adjust military capability and preparedness in response to emerging challenges. This includes the supply of specialised munitions and logistic requirements, such as fuel, critical to military capability.'[14]

Complementing the strategic forecasts of the DSU, the updated FSP provided significant capability funding to meet the future challenges. It included a commitment to allocate approximately $270 billion investment in defence capability in the decade to 2029-30.

Importantly, both the DSU and FSP recognise that supply chains are critical to Defence capability. The DSU also noted that our changing world and increased reliance on technology and connectivity has a profound effect on the vulnerability of supply chains:

'The increasing connectivity of services and infrastructure to the internet will expose vulnerabilities in global supply chains, critical infrastructure and support services. These will be key targets in grey-zone activities and as a precursor to conventional conflict. The challenge of protecting critical technologies from intellectual property theft will become harder and will have major security as well as economic impacts.'[15]

The FSP also contains a line of funding for 'Supply Chain Upgrades' valued at between $2.3 billion and $3.5 billion, with funding commencing in 2030. This is equivalent to 0.9-1.2 per cent of the $270 billion of capability investment identified in the FSP. While this additional resourcing is welcome, whether this quantum is sufficient to address supply chain vulnerabilities remains an open question, as the extent of these vulnerabilities is yet to be fully mapped. In addition, the funding is not scheduled to commence until 2030. Further deteriorations in the geostrategic environment may require this resource allocation to be increased and/or brought forward in Defence's investment plans.

Defence structures and strategies to help secure supply chains

Defence has undertaken a range of activities to implement additional security measures for supply chains. At present, there are several bodies within Defence responsible for helping to secure supply chains:

- Joint Logistics Command (JLC) has responsibility for the planning, coordination and delivery of military logistics for Defence, including defence supply chains (warehousing, distribution, material maintenance and retail store services).
- The Capability, Acquisition and Sustainment Group (CASG) have undertaken supply chain assessments for some large Defence capabilities and uses the Supply Network Analysis Program (SNAP) tool to assist with these assessments (discussed further below).
- Defence Industry Policy Division has carriage of defence industry policy, including development of the policies relating to Sovereign Industrial Capability Priorities (SICPs).
- Other groups in Defence also play a role in protecting supply chains, such as Defence Security and Estate, which manages the Defence Industry Security Program (DISP).
- Various groups develop planning guidance within Defence, some at the classified level, providing direction on the security of supply chains.

Various parts of Defence play an important role in supply chain security. However, no one area in Defence has full policy responsibility for the development of strategy, risk assessment, and risk mitigation for defence supply chains.

More broadly, the previous federal Government established structures and initiatives to strengthen Australia's supply chain resilience, including the Office of Supply Chain Resilience (now within the Department of Industry, Science and

Resources) and Cabinet. It will be important that any Defence activities link in with these broader initiatives and support inter-agency collaboration and co-operation.

Defence's use of the SNAP tool in supply chain risk assessment

Defence has invested significant resources into the acquisition and deployment of automated tools to help understand supply chains through data analytics. The Defence Supply Network Analysis Program (SNAP) is a Defence framework for supply chain mapping. It uses a commercially available software tool and open-source data to map defence supply chains across multiple tiers of providers. The software tool uses machine learning and data analytic methods to process this data and create an approximated 'map' of the full defence supply chain. Human analysis then evaluates and acts upon this data. SNAP has been piloted on a number of defence platforms, delivering new insights not hitherto available to Defence.

The advantages of the SNAP tool are two-fold. First, it provides far greater depth – mapping supply chains back over multiple tiers – than existing supply chain management practices reveal. This is particularly useful in identifying 'diamond' and 'hourglass' supply chain risks that are not immediately visible. Second, as an automated tool it is far more resource-efficient than current (human-conducted) supply chain studies. This will allow SNAP to scale from pilot studies to defence-wide use far more easily than prior methods.

In line with the *Defence Data Strategy*, CASG has noted that it needs to move away from using data as a rear-view mirror, and towards integrating analytics directly into its daily decision-making. It states:

'*[SNAP] will provide Defence visibility of its supply chains, making them more transparent across multiple tiers. By doing so, Defence will be better equipped to understand the specific risk lens that apply to our supply networks – be it financial, operational or geopolitical – and actively monitor red flags as they arise in real-time.*'[16]

Defence has stated that it is investigating how it can effectively, securely and ethically share the insights it gains into its supply chains, and Defence has noted that this work is ongoing.

Sovereign Industrial Capability Priorities and links to supply chains

The 2018 *Defence Industrial Capability Plan* can also support the supply chain security agenda, through plans for development of the Australian industrial base and the Sovereign Industrial Capability Priorities (SICPs).

SICPs are capabilities that are critical to Defence and must be developed or supported by Australian industry. This means Australia must have access to, or control over the skills, technology, intellectual property, financial resources and infrastructure that underpin each. The SICPs are industrial capabilities that Defence relies on to deliver its core objectives, and will be managed closely across defence and industry planning.

The development of the SICPs should be closely linked to supply chain security. However, the current list of SICPs released by Defence is extremely broad, covering a wide range of Defence capabilities. Ten SICPs were announced in 2018:

- Collins Class Submarine maintenance and technology upgrade;
- Continuous Shipbuilding Program (including rolling submarine acquisition);
- Land Combat Vehicle and technology upgrade;
- Enhanced Active and Passive Phased Array Radar Capability;
- Combat clothing survivability and signature reduction technologies;
- Advanced signal processing capability in Electronic Warfare, Cyber and Information Security, and Signature Management technologies and operations;
- Surveillance and intelligence data collection, analysis, dissemination and complex systems integration;
- Test, evaluation, certification and systems assurance;

- Munitions and small arms research, design, development and manufacture; and
- Aerospace platform deep maintenance.

A further four SICPs were added in 2021:

- Robotics, Autonomous Systems, and Artificial Intelligence;
- Precision Guided Munitions, Hypersonic weapons, and Integrated Air and Missile Defence Systems;
- Space; and
- Information Warfare and Cyber Capabilities.

The implementation plans for the SICPs have been developed incrementally in Defence since 2018, and there are now eight plans released, with another six on the way.

The SICP implementation plans should be fully integrated with Defence's risk assessment and risk mitigation measures for critical defence supply chains. However, due to the breadth of the SICPs, as well as a lack of a whole-of-Defence approach to supply chain security, a cohesive and integrated risk assessment and risk mitigation process for our sensitive technologies has not yet been established. This is also due, in part, to the lack of a central coordinating body for the development of supply chain security policy and risk mitigation strategies within Defence.

Future plans under the federal Government

The federal Government has released plans for the development of Defence, including:

- A new Force Posture Review, which will look at how the Australian Defence Force (ADF) assets and personnel are positioned to deal with the current and future strategic circumstances for Australia and the Indo-Pacific region;
- A Defence Industry Development Strategy; and
- Establishment of an Australian Strategic Research Agency.

All of these activities present opportunities to embed supply chain security initiatives, such as those recommended in this report, into the Australian Defence and defence industry context.

5 Current supply chain practices in the Australian defence sector

Given the need to manage new and emerging risks, how do current supply chain practices in the Australian defence sector align to the resilience agenda?

Assessing the security of defence supply chain practices is a challenging task, as information is not routinely made available. Data on the structure of supply chains managed by Defence Primes is often commercial-in-confidence; while for many sensitive or high-technology platforms security requirements further restrict the availability of information. While the protection of information on supply chains is entirely appropriate for the defence sector, it increases the difficulty of assessing current approaches against their ability to deliver security and resilience.

To generate insights into current Australian practices, this project conducted consultations with a range of Defence and defence industry stakeholders. These consultations generated qualitative insights into the nature of Australian defence supply chains, current supply chain management practices, the impact of both traditional and strategic risks presently facing the sector, and emerging resilience efforts emanating from both government and industry. These consultations generated the following findings regarding the contemporary state of play for defence supply chain security.

Visibility of defence industry supply chains

The availability of accurate and detailed information on supply chains is a precondition for effective approaches to security. Yet Australian Defence and defence industry participants reported that a comprehensive picture is not available to stakeholders. A consistent approach or methodology for mapping supply chains, which is mutually agreed between Defence and defence industry, also does not exist.

Several industry participants reported that they have a good understanding of their supply chains down to the second or third tier. These are developed as part of their normal supply chain management practices. This is considered sufficient for commercial purposes by industry standards, and provides sufficient visibility to anticipate and mitigate traditional risks. But for practical reasons, visibility does not extend consistently to deeper tiers, particularly back to the tiers where strategic supply chain risks may emerge.

In recent years, Defence has committed to increasing the visibility of defence supply chains, and has initiated several programs to build informational resources. These include:

- Use of the Supply Network Analysis Program (SNAP) tool to more deeply map supply networks and identify resultant risks and opportunities for selected platforms and critical materiel with enterprise-wide impacts;
- A renewed focus on supply chain security by Joint Logistics Command;
- The establishment of an economics team in Defence Industry Policy division; and
- A focus on supply chains by the recently established Office of Defence Industry Support.

The Defence Industry Security Program (DISP) also provides security vetting for Australian businesses in defence supply chains, and therefore acts as a form of supply chain security. However, DISP has a different purpose and function to protecting supply chains against strategic risks and is unlikely to cover goods and services beyond the first several tiers in a defence supply chain.

There was evidence from Defence, confirmed during the consultation process, that more detailed investigations have found 'diamond' supply chains behind some of Australia's key defence platforms. As concentration in diamond supply chains occurs many stages back from the final consumer, these are not routinely identified by normal supply change management practices. These pose a hitherto unidentified supply chain risk. As these investigations have only been undertaken on a pilot or exploratory basis for select platforms, the extent to which diamond supply chains occur across Defence remains unknown.

In terms of defence industry, some Defence Primes have begun undertaking supply chain mapping at a more detailed level than previously. This has revealed important sourcing information, and in some cases been useful in identifying areas where new Australian Industry Capability has been developed. Several large industry participants noted the implementation of the recent modern slavery legislation had opened up some further visibility of their supply chains. There is, however, no evidence of the widespread use of commercial tools within industry to map and identify strategic risks in supply chains. While these may be used overseas in the global parent companies, the use of commercial supply chain tools does not appear to be standard practice in Australian industry.

Traditional vs strategic supply chain risks

Industry participants reported that managing traditional – commercial and logistics – risks dominates supply chain security efforts. Procurement specialists noted that they spend significant effort and energy ensuring continuity of supply, efficient delivery timeframes and cost efficiency for delivery of capability. Commercial, logistic, schedule and cost issues were key drivers in terms of managing supply chains for both larger and smaller companies.

The COVID-19 pandemic has intensified this bias in recent years, as a result of placing additional pressure on shipping costs, schedule delays and the competition for raw materials and intermediate components. Semiconductors, presently in very short supply due to the global semiconductor crunch, was the most pressing challenge, but shortages are reported across all areas of the supply chain. The increased cost of freight and long delivery timeframes were examples of service linkage (rather than material shortages) that were also affecting supply chain integrity.

COVID-induced supply chain difficulties were reported by both Prime and SME participants, reflecting the global and systemic nature of the problem. However, SMEs are especially exposed and report that they must prioritise cost incentives to participate in larger supply chains. Cost then becomes the priority over strategic considerations such as source and location of supply.

By contrast, strategic risks have received comparatively less attention. These are an increasing source of concern for Defence and industry, but remain a more recent addition to the supply chain agenda and lack the clarity of focus of other commercial and logistic risks. This partially reflects the challenges posed by COVID-19 interruptions, which have in the last two years consumed much of resources available for supply chain management.

However, this is beginning to change. As noted prior, Defence has undertaken a range of new activities focussed on strategic risks to supply chains, while industry is also taking measures in individual cases. These efforts could be accelerated with changes to the interactions between government and business. Several participants noted the importance of Defence making strategic supply chain risk a priority in contracts, and balancing its importance against other commercial outcomes during the procurement process.

The relationship between Defence and defence industry

Defence and defence industry participants all reported that efforts to address supply chain security are presently being augmented, in light of both rising traditional and emerging strategic risks. However, consultation also revealed there were differences between how Defence and defence industry are approaching this task.

Participants reported that there are overlapping frameworks for identifying supply chain risks. Several Prime representatives stated that significant supply chain security activities occurred in their parent corporations – that work was completed overseas rather than locally in Australia, including the use of commercial tools.

A potential disconnect was also reported at the link between acquisition and sustainment activities: that supply chain security efforts were individually undertaken in each of the two stages. Supply chain management plans are put in place during the acquisition phase, but then a separate and distinct set of plans would be deployed during sustainment, often as a result of 'carriage' of a platform being transferred between parties on either the Defence and/or industry side. This approach means there is sometimes a lack of continuity in supply chain management practices across the life cycle of a capability.

Several participants argued that collaboration between Defence and defence industry – while already an established practice – could be strengthened to deliver better commercial and policy outcomes. Suggested avenues included:

- Developing an agreed set of definitions and standards for supply chain security issues.
- Applying a consistent approach to supply chain security across different defence platforms, so that companies participating across multiple platforms can operate within a single framework.
- Clarifying roles and responsibilities for Defence and defence industry in identifying, risk-assessing and mitigating supply chain vulnerabilities.
- Sharing of information on vulnerabilities – including those generated by automated tools – with industry where appropriate.
- Developing a list of 'certified suppliers' that would identify "trusted" partners within a supply chain.
- More fully incorporating supply chain management practices in contracting and procurement.
- Addressing supply chain issues in the very early stages of the project life-cycle, so these can be considered alongside cost and capability considerations. A framework would need to be developed to identify thresholds to ensure this is cost effective.
- Further developing the concept of industry as a 'fundamental input to capability' to ensure that formal consideration is given to industry capability and capacity (including supply chains) earlier in the capability life cycle.

6 International responses to defence supply chain vulnerabilities

Australia is not alone in facing challenges for the security of defence supply chains. Many governments around the world – including the US, UK, Japan, India, South Korea and Taiwan – have begun similar steps to investigate supply chain risks, and strategically invest in mitigation and resilience. The US and UK have taken these initiatives the furthest, and sit roughly at the same position as Australia in terms of new policy and strategy development. We note the defence supply chain initiatives of these countries share some common themes:

- Efforts to assess defence supply chain risks are very recent for most governments, with the UK and US undertaking comprehensive and deeper assessments of their supply chain vulnerabilities and resilience.
- The defence industry issues identified by these governments are structurally similar to those identified by Australia – namely, a reliance on global supply chains whose security is under pressure from both traditional and strategic risks.
- The US and UK have specifically deployed policies relating to supply chains for defence industry and critical goods. These are particularly relevant for Australia, given their efforts are at a similar stage of development, and the close defence industry ties established with the AUKUS agreement.
- All four Quad countries now have defence supply chain security policies in place, as well as South Korea and Taiwan (the other major US treaty partners in Asia). However, in comparison to the US, UK and Australia, their efforts are at an earlier stage of development.

The United States

The United States has been undertaking comprehensive evaluation of their supply chain risks, vulnerabilities and resilience. In the civilian economy, the initial focus has been on four critical products: semiconductors, large capacity batteries, critical minerals, and pharmaceuticals ingredients[17]. Separately, the US House Armed Services Committee has been leading assessment into supply chain risk and resilience in the defence context, with

input from leading industry experts and representatives, and current and former US Department of Defense officials[18].

The proximate driver of these reviews has been the COVID-19 pandemic[19]. The impact of the pandemic has led to economic dislocation and highlighted long standing strategic supply chain vulnerabilities and national security risks. However, the pandemic has also amplified long term issues in the US defence industrial base. These have been attributed to the steady US deindustrialisation over a long period of time, end of the Cold War, advancements in high-tech and digital technologies, and the rising military and economic threat of China[20]. The review found that it was difficult to have sufficient visibility on the defence supply chain (including where material and supplies are sourced and manufactured)[21]. This was critical to enable a better understanding of its current vulnerabilities and surge capacity, and in order to build resilience and mitigating risk.

The US recommended legislative reforms to address the specific challenges for the defence supply chain[22]. These include requiring the supply chain security to be treated as a defence strategic priority, requiring tools to enable visibility on the defence supply chain, requiring identification of supplies and materials from and reducing reliance on adversarial countries, strengthening and developing closer collaboration with allies through the National Technology and Industrial Base (NTIB), and supporting research, development and innovation initiatives related to rare earth elements in the supply chain.

The United Kingdom

In 2021, the UK Defence Committee undertook an extensive inquiry into vulnerabilities of their defence and security supply chain. Similar to the US, this review was driven by the COVID-19 pandemic. The inquiry particularly focussed on the extent of foreign ownership and government intervention powers, impact of the pandemic on supply chains (particularly SME finances), additional protection measures required and international lessons from allies[23].

The inquiry found it was difficult to define foreign involvement in the UK defence supply chain. Despite this, the inquiry considered that there were current risks to foreign influence for foreign domiciled companies and global supply chains for defence were vulnerable especially where materials are sourced from those not aligned with the UK. It argued that there was also insufficient oversight of the defence supply chain to assess risks and recommended identification of only friendly countries that can invest in the UK defence supply chain.

There was also particular concern about defence supply chain companies (especially SMEs and commercial aerospace) facing financial pressures due to the pandemic, leading to increased risk of hostile foreign influence. Measures recommended in the inquiry included providing better support for defence sector and commercial aerospace industry during the pandemic and for SMEs to engage in UK Defence work.

Nevertheless, recognising global supply chain vulnerability, the UK Government noted that its review of the Defence and Security Industrial Strategy included prioritising sovereign capability within the UK defence industry, mapping of critical supply chains and considering what should be directly available in the UK. It also acknowledged its diverse global trading partners involved in its critical supply chains and collaboration with allies including via the NTIB that includes Australia.

Other regional partners – Japan, India, South Korea and Taiwan

The Japanese Ministry of Defense (MoD) has intensified its supply chain security efforts since 2019, beginning with a survey of 68 major defence equipment items in 2019. As a result of this survey's findings, the MoD has adopted a number of policies designed to increase the security of defence supplies across the supply chain (i.e. behind the Prime contractors). This included reforming contracting to encourage a wider range of suppliers into supply chains, building a regular monitoring system for early risk identification, and

identifying SMEs that have desired technologies or products to fill supply chain gaps. The MoD has also started direct engagement with *Keidanren* (the Japanese business federation) and its defence industry members on methods for greater government-business collaboration for supply chain security[24].

The Indian Ministry of Defence has outlined a range of specific defence activities to move towards a "self-reliant India" to enhance India's domestic manufacturing, and become a net exporter in defence materiel[25]. This has included: giving major priority to locally-made products as part of the planning and procurement of Indian Army equipment; handing over of six Transfer of Technology agreements to seven public and private sector companies; and converting the Ordnance Factory Board into seven new government-owned defence manufacturers. Complementing this, the Indian Government announced "self-sufficiency" measures in Indian defence investment, earmarking 68 per cent of the capital procurement budget for domestic industry in equipment for the Indian Armed Forces in 2022-23, and 25 per cent of the defence R&D budget[26].

The South Korean Government is planning to open the Economic Security Center under the Ministry of Foreign Affairs, focussed on securing supply chains for critical goods and emerging trade issues[27]. The South Korean Government's measures to strengthen its economic risk management also include launching a taskforce to secure important materials supply, building an early warning system of 4,000 items sensitive to supply risk, and determining a list of 200 products that are classified as critical for national security needs. The Head of the Defence Acquisition Program Administration has indicated that South Korea has begun exploring joint defence supply chain initiatives with the US[28].

In May 2022, the Taiwanese Government announced to promote six 'Core Strategic Industries' to "*gain first-mover advantage to capitalize on opportunities in the post-pandemic era created by the reorganization of global supply chains*"[29]. Of particular interest, national defence and strategic industries have been identified as a priority area, covering: the aerospace and shipbuilding industries in terms of self-maintenance, military-civil cooperation and international certification; and the space industry focussed on developing low-Earth orbit satellites and ground stations and support equipment[30]. The Taiwanese Government has also developed a *National Development Plan* for 2021-2024, prioritising national defence reform to enable national defence self-sufficiency, with actions to consolidate technological capabilities and promote the national defence industry[31].

7 Framework principles for secure defence supply chains

Supply chain security is not a new issue for the Australian defence sector. But it has become more challenging and is likely to become more so in future. Since the beginning of the COVID-19 pandemic, interruptions to global supply chains have steadily mounted, affecting all sectors of the economy including defence.

A deteriorating geostrategic environment has made strategic supply chain risks – hitherto less a direct challenge – far more likely to occur. While it remains to be seen when traditional supply chain risks return to normal levels, there is every reason to expect that heightened strategic risks will become a structural feature of the defence sector for years to come.

As foreshadowed in the 2020 *Defence Strategic Update*, now is the time to upgrade the frameworks and practices for supply chain security in the Australian defence sector.

However, there is no one-size-fits-all solution for defence supply chain security. There is considerable diversity amongst defence supply chains in terms of their geometry, the presence of critical nodes, and their exposure to both traditional and strategic risks. There are also a range of options for managing these risks, ranging from low-cost but scalable solutions such as diversification and stockpiling, through to potentially higher cost but more impactful options like developing trusted or sovereign capabilities.

As the resources available to address supply chain security are finite, the agenda must be an exercise in risk management: identifying and measuring risks, and deploying targeted and proportionate responses where required.

Moreover, ensuring supply chain security is a 'whole of defence' endeavour. There is naturally a leading role for the federal Government, particularly the Department of Defence and ADF as the buyer, manager and end-user of defence equipment and materiel. But defence industry has an equally critical role to play, given its deep knowledge of defence supply chains and expertise in supply chain management. This importance extends beyond the Defence Primes, to include key corporate players in the upper tiers of the supply chain as well. Security initiatives need to be designed in a manner that engages the entire defence industry ecosystem, to work together toward the common goal of more resilient global supply chains.

To support this agenda, we propose a set of 'framework principles' that can help new defence supply chain security efforts

FIGURE 4: FRAMEWORK PRINCIPLES FOR DEFENCE SUPPLY CHAIN SECURITY

Informational resources	• Map supply chain geometry to identify critical nodes • Assess current and future flexibility requirements • Include supply chain at start of project life cycle
Assigning risk	• Identify nodes facing above-normal traditional risks • Assess likelihood and impact of strategic risks • Forecast risk assessments over project life
Calibrating interventions	• Analyse and assess interventions: stockpiling or diversification strategies • Build trusted capability networks • Develop sovereign capability
Government – industry collaboration	• Agree definitions and shared understanding of supply chain concepts • Establish governance and mechanisms for information sharing • Incorporate supply chain security into contracting

between Defence and defence industry. Four principles – regarding *informational resources*, *assigning risk*, *calibrating interventions* and *government-business collaboration* – are identified as critical for achieving effective supply chain security practices (Figure 4). While the implementation of these principles will naturally vary between different defence supply chains, they provide a strategic framework that can guide the development of future policy.

Developing effective informational resources is the first step in effective supply chain security practices. Currently, information on the structure of defence supply chains is variable, fragmented between different parts of Defence and defence industry, and not of sufficient resolution to fully identify vulnerabilities. The extent to which a particular supply chain is mapped will be dependent on an assessment of criticality and a cost-benefit analysis, given supply chain mapping is a costly endeavour. Nevertheless, developing stronger informational resources is the foundation for all defence supply chain resilience initiatives. This can be achieved by:

- *Extended mapping of supply chain geometries to identify critical nodes*. Mapping of supply chains is the first step required to identify whether, and where, critical nodes exist. Given the extended nature of defence supply chains – often over ten links deep – this mapping exercise needs to go back significantly further than conventional supply chain management practices. Automated software tools provide a new method to undertake these mapping exercises in greater detail, and in a more timely and cost-effective manner than previous human-conducted mapping.

- *Assessing current and future flexibility requirements.* Defence supply chains need to meet two sets of performance criteria: supporting current operational requirements, while also having 'surge capacity' to scale up quickly as future strategic circumstances require. Supply chains which are found to be resilient against the former criterion may not be for the latter. Supply chain mapping should seek to identify critical nodes against both current operational needs and planned-for future scenarios.
- *Including supply chain at the start of project life cycle.* Given the technological sophistication of contemporary defence platforms, supply chain structures are determined early in a project's life cycle. As many defence capabilities have few or only one global supplier, the act of choosing to acquire a capability often carries with it the need to use a particular supply chain. As a consequence, supply chain considerations need to be brought forward in the project life cycle, to ensure the supply chain implications of early stage decisions are considered before they are made.

Establishing a framework for assigning risk to identified critical nodes. While mapping exercises identify the location of critical nodes within a supply chain, they do not assess the level of risk at these nodes. Subsequent risk assessment exercises are required to estimate the likelihood of an interruption occurring at a node, and identifying the impacts that an interruption would carry on supply chain resilience. These risk assessment exercises cannot be easily automated, as they require qualitative (i.e. human) evaluation of current and future risk profiles. Risk assessment should:

- *Identify nodes facing above-normal traditional risks.* While traditional supply chain risks can affect any stage, some nodes are more exposed to interruption than others. Attention should be directed to those which are highly vulnerable to traditional risks. These include products with specific technical requirements that prevents substitution to new suppliers during an interruption, and those where there is competition with civilian users. Attention should also be directed to intangible supply chain links – such as access to personnel with specialised skills – that can also be affected by interruptions.
- *Assess likelihood and impact of strategic risks.* While strategic supply chain risks are yet to directly affect defence supply chains, changes in Australia's geopolitical environment mean they may credibly occur in coming years. Risk assessments must therefore also include a political risk component, which considers the likelihood of geopolitical developments inhibiting supply chains. Strategic risks must also be weighed against their impact on supply chain integrity.
- *Forecast risk assessment over project life cycle.* Both traditional and strategic supply chain risk factors can change suddenly. The long life cycle of defence capabilities and platforms – usually measured in decades – means that static risk assessments will fail to capture over-the-horizon vulnerabilities. Assessments must therefore also forecast the likelihood of supply chain risks over the entire project life cycle, not simply under current parameters.

Calibrating supply chain interventions to the identified risk. While there are many interventions which can be used to improve supply chain resilience, all impose costs relative to status quo practices. It is therefore important to match interventions to their identified risk, using lower-cost options for mild to moderate risks, and reserving higher-cost interventions for the most serious risks. General principles include:

- *Use stockpiling and diversification strategies where effective.* These are usually the lowest-cost supply chain interventions, and therefore should be used as a first-resort where they can effectively mitigate identified risks. Stockpiling requires no change to supply chain structures and can insure against traditional risks that are temporary in nature. Diversification can provide flexibility against both traditional and strategic risks for nodes with low to moderate criticality.

- *Build trusted capability networks where required*. Where a component is sufficiently critical that it demands greater security than standard supply chain practices, trusted capability networks provide an effective middle ground. Utilising trusted partners with established capabilities can be an effective solution and allows finite resources to be deployed against a wider number of supply chain threats. It also allows access to foreign technology and skills, which may not be practicably transferrable to Australia for commercial and/or security reasons.
- *Build sovereign capability where effective and required*. Sovereign capability is the most secure supply chain resilience intervention, yet potentially has greater up-front costs. It can also prove time-consuming to establish local capabilities relative to other options. Sovereign capability should be developed as appropriate following detailed review of supply chain risks – usually those of a strategic nature. Assessing whole-of-life costs, not just initial acquisition costs, is an important part of determining the cost-effectiveness of this strategy.

Build deeper government-industry collaboration. Supply chain resilience is a shared government-business agenda. While Defence plays a leadership role as policymaker and customer, defence industry – in Australia and overseas – has a critical role in both identifying risks and implementing resilience measures. It is therefore crucial to have mutual and effective mechanisms for government-industry collaboration, which will need to extend deeper than current practices. Some of the most important forms comprise the following:

- *Agreed definitions and shared understanding of supply chain concepts*. Defence and defence industry must be 'on the same page' when collaborating for supply chain resilience. There needs to be mutually agreed definitions of key supply chain concepts – particularly around what constitutes 'critical' – and a shared understanding of the appropriate types and level of information required. These concepts need to be mutually agreed between Defence and defence industry, so that they are practicable for both sides.
- *Establish governance and mechanisms for information sharing*. There is a need to better share information between and within Defence and defence industry on the structure of supply chains and identified risks. However, this sharing process also poses important governance questions, concerning both commercial- and security-sensitive information. A governance framework that addresses how information should be managed, and mechanisms for its sharing under appropriate circumstances, is a critical precondition for deepening government-business collaboration. A key concept will be the development of inter-agency co-operation and collaboration to support the resilience of supply chains across the commercial and defence sectors. This would also build on the work of the Office of Supply Chain Resilience.
- *Incorporate supply chain security into contracting*. Decisions made at the very earliest stages of defence procurement processes carry implications for supply chain security. However, many procurements only minimally address supply chain matters at acquisition and/or defer them to the sustainment stage. Supply chain security issues must be front-ended in defence procurement processes and contracts designed to explicitly address the role of Defence and defence industry, as per the intent of industry as a 'fundamental input to capability'. An important consideration is how costs are shared, particularly where supply chain adjustments are required mid-way through the project life cycle.

8 Policy recommendations

1 Defence to develop a comprehensive strategy and action plan in relation to the strategic protection of defence supply chains. This should include:

- Making a declaration that supply chain resilience is a strategic priority for Defence and defence industry;
- Providing a central coordinating area within Defence with full policy responsibility for supply chain issues; and
- Developing a clear, transparent and agreed supply chain protection policy, including risk assessment frameworks and options for intervention, developed in partnership with industry.

2 Strengthen supply chain considerations into the full Defence capability life cycle and decision-making, including within the following:

- Capability development, acquisition and sustainment programs across the organisation;
- Defence Industrial Capability Plan and Sovereign Industrial Capabilities Priorities;
- Defence Industry Security Program; and
- Defence innovation programs, including the Defence Innovation Hub and the Next Generation Technology Fund.

3 Establish robust and scalable mechanisms for generating information on defence supply chain risks.

This includes programs for mapping existing and future supply chains, risk assessment toolkits for assigning priority to identified vulnerabilities, and the use of commercial tools where appropriate in both Defence and defence industry.

4 Establish governance structures that allow regular and organised engagement with industry.

This includes both information sharing mechanisms for the identification and reporting of vulnerabilities, and consultation mechanisms for developing mitigation measures. This reporting and information sharing should include information that is generated via the use of commercial supply chain tools such as the Supplier Network Analysis Program (SNAP).

5 Review and develop appropriate resourcing for supply chain resilience initiatives.

Increased strategic supply chain risks will necessitate a greater allocation of resources, with the quantum and form of resourcing to be determined as new risk assessment exercises generate better information. Resourcing requirements will also need to be factored into contractual arrangements with industry.

6 Develop a clear methodology to identify, select and resource supply chain interventions to identified risks.

Approaches to intervention should be reviewed in detail following a risk assessment, including options for:

- Building strategic reserves/inventories/stockpiling;
- Increasing diversity in the supplier base;
- Prioritising the inclusion of trusted partners in supply chains; and
- Developing sovereign capabilities, which may range from critical components through to full local manufacture.

7 Increase the priority accorded to supply chain issues during defence procurement processes calibrated by risk.

Supply chain issues need to be considered at the very start of the project life cycle (as part of industry as a fundamental input to capability) and systematically incorporated into project development, acquisition, contracting and sustainment. Given the rapidly changing strategic environment, flexibility will need to be built into how supply chain issues are contracted.

8 Collaborate with international partners to enable trusted-capability supply chain options.

This includes government-to-government engagement, with a particular focus on the US and UK (particularly leveraging AUKUS) and other likeminded partners undertaking their own supply chain security programs. It also includes ensuring industry partnerships engage both with Australian defence industry and international industry partners.

9 Create a structure for inter-agency collaboration on supply chain resilience initiatives.

Overlaps between defence and civilian supply chains mean there are benefits from aligning resilience initiatives across the two domains. Establishing mechanisms for inter-agency collaboration will ensure that efforts undertaken in broader domains of the economy can support defence supply chains, and vice versa.

Acknowledgements

During the execution of this project, members of the Defence Council and broader industry were consulted in the development of this report. Ai Group and Perth USAsia Centre would like to extend our thanks for their insights and support. We would also like to thank the wide range of individuals who have supported this project. Kate Louis and Jeffrey Wilson led the project team, supported by Louise McGrath, Charles Hoang, James Scotland and Cathrine Whitmore of Ai Group, and Gordon Flake, Hayley Channer, Gemma King and Emily Davies of Perth USAsia Centre. Many other individuals – across business, government and industry – kindly offered insights, information and feedback that have enriched the project. We especially thank Wayne Cooper of the Department of Defence for his support. Nonetheless, Ai Group and Perth USAsia Centre are responsible for all content and arguments contained herein.

AiGROUP
DEFENCE COUNCIL

About the Australian Industry Group

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for nearly 150 years. Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than one million staff. Our members are small and large businesses in sectors including manufacturing, construction, engineering, transport & logistics, labour hire, mining services, the defence industry, civil airlines and ICT. Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

Perth USAsia Centre

About the Perth USAsia Centre

The Perth USAsia Centre located at The University of Western Australia is a non-partisan, not-for-profit institution strengthening relationships and strategic thinking between Australia, the Indo-Pacific and the US. The Centre is a leading think tank focussing on geopolitical issues, policy development and building a strategic affairs community across government, business and academia. Since the Centre's inception in 2013, we have collaborated with over 40 partners to convene more than 400 programs across 16 cities in eight countries, engaging a world-class community of over 10,000 strategic thinkers and policy leaders.

This research was supported by the Australian Government through a grant by the Australian Department of Defence. The views expressed herein are those of the authors and are not necessarily those of the Australian Government or the Australian Department of Defence.

References

1 Department of Defence (Australia) (2020), *Defence Strategic Update 2020*, p. 16, https://www.defence.gov.au/about/publications/2020-defence-strategic-update.

2 In Australia, eight "Prime contractors" currently participate in the Department of Defence's Global Supply Chain Program (GSCP). See https://www.defence.gov.au/business-industry/industry-programs/global-supply-chain. Other large companies are growing in Australia, adding to the number of Primes within the defence industry.

3 For the foundational definition of criticality, see US National Academies of Science (2009), *Minerals, Critical Materials and The US Economy*, Washington DC: The National Academies Press, https://www.nap.edu/catalog/12034/minerals-critical-minerals-and-the-us-economy. In the Australian context, the Productivity Commission has adopted a similar definition to assess supply chain vulnerability. See Productivity Commission (Aus) (2021), *Vulnerable Supply Chains*, https://www.pc.gov.au/inquiries/completed/supply-chains/report/supply-chains.pdf.

4 McKinsey (2021), *Coping with the auto-semiconductor shortage: Strategies for success*, 27 May, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/coping-with-the-auto-semiconductor-shortage-strategies-for-success.

5 Supply Chain Dive (2021), 'Timeline: How the Suez Canal blockage unfolded across supply chains', 6 July, https://www.supplychaindive.com/news/timeline-ever-given-evergreen-blocked-suez-canal-supply-chain/597660/.

6 Bloomberg (2021), 'Clearing U.S. Port Congestion Turns Into a Game of Whac-a-Mole', 16 December, https://www.bloomberg.com/news/newsletters/2021-12-16/supply-chain-latest-clearing-u-s-port-congestion-turns-into-whac-a-mole.

7 The Economist (2021), 'Why supply-chain snarls still entangle the world', 18 December, https://www.economist.com/business/a-return-to-container-shippings-pre-pandemic-days-is-a-long-way-off/21806844.

8 Wall Street Journal (2021), 'The Chip Shortage Is Bad. Taiwan's Drought Threatens to Make It Worse', 16 April, https://www.wsj.com/articles/the-chip-shortage-is-bad-taiwans-drought-threatens-to-make-it-worse-11618565400.

9 Reuters (2021), 'Japan's Renesas sees fire-damaged chip plant back to full capacity by mid-June', 1 June, https://www.reuters.com/technology/renesas-restore-fire-hit-chip-plant-100-capacity-around-mid-june-2021-06-01/.

10 Wall Street Journal (2022), 'Kazakhstan Unrest Pushes Up Uranium and Oil Prices', 6 January. https://www.wsj.com/articles/kazakhstan-unrest-pushes-up-uranium-and-oil-prices-11641497655.

11 Australian Financial Review (2021), 'MUA suspends Fremantle Port strikes ahead of federal intervention', 15 October, https://www.afr.com/work-and-careers/workplace/mua-suspends-fremantle-port-strikes-ahead-of-federal-intervention-20211015-p59079.

12 Jeffrey Wilson (2021), 'Australia Shows the World What Decoupling From China Looks Like', Foreign Policy, 9 November, https://foreignpolicy.com/2021/11/09/australia-china-decoupling-trade-sanctions-coronavirus-geopolitics/.

13 Marcus Hellyer (2021), *The Cost of Defence: ASPI defence budget brief 2021–2022*, Australian Strategic Policy Institute, https://www.aspi.org.au/report/cost-defence-aspi-defence-budget-brief-2021-2022.

14 Department of Defence (Aus) (2020), *2020 Defence Strategic Update*, https://www.defence.gov.au/about/publications/2020-defence-strategic-update, p. 14.

15 Ibid.

16 Department of Defence (Aus) (2021), *Defence Data Strategy 2021-2023*, https://www.defence.gov.au/about/publications/defence-data-strategy-2021-2023, p. 40.

17 White House (US) (2021), *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017*, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

18 House Armed Services Committee (US) (2021), *Report of the Defense Critical Supply Chain Task Force*, p. 9, https://armedservices.house.gov/_cache/files/e/5/e5b9a98f-9923-47f6-a5b5-ccf77ebbb441/7E26814EA08F7F701B16D4C5FA37F043.defense-critical-supply-chain-task-force-report.pdf.

19 White House (US) (2021), *Executive Order on America's Supply Chains*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/; House Armed Services Committee (US) (2021), *Report of the Defense Critical Supply Chain Task Force*, p. 5.

20 House Armed Services Committee (US) (2021), *Report of the Defense Critical Supply Chain Task Force,* p. 5.

21 Ibid, p. 3.

22 Ibid, pp. 16-18.

23 Defence Committee (UK) (2021), *Foreign Involvement in the Defence Supply Chain*, Fourth Report of Session 2019-21, # HC 699, pp. 5, 30-32, https://committees.parliament.uk/publications/4733/documents/48029/default/; and UK Government (2021), *Appendix: Government Response*, Fifth Special Report of Session 2019–21, https://publications.parliament.uk/pa/cm5801/cmselect/cmdfence/1380/138002.htm.

24 Ministry of Defense (Japan) (2021), *The Defence of Japan 2021*, https://www.mod.go.jp/en/publ/w_paper/index.html.

25 Indian Government (2021), *Year End Review – 2021 of Ministry of Defence*, 31 December, https://pib.gov.in/PressReleasePage.aspx?PRID=1786640.

26 Indian Government (2022), *Union Budget 2022-2023, Speech of Minister of Finance*, 1 February, p. 15, https://www.india.gov.in/spotlight/union-budget-fy-2022-2023.

27 *Yonhap* (2022), 'S. Korea to launch economic security center in March', 31 March, https://en.yna.co.kr/view/AEN20220128001800325.

28 *Yonhap* (2022), 'Arms agency chief says S. Korea open to joining U.S. defense supply chains', 11 February, https://en.yna.co.kr/view/AEN20220211006400325.

29 National Development Council of Taiwan (2020), *Program for Promoting Six Core Strategic Industries,* https://www.ndc.gov.tw/en/Content_List.aspx?n=2D827BFE7E3598BE.

30 National Development Council of Taiwan (2021), *National Development Plan (2021-2024)*, https://www.ndc.gov.tw/en/Content_List.aspx?n=9649AD857AF274BA, pp. 23-24.

31 Ibid, pp. 76-77.

AIGROUP
DEFENCE COUNCIL

Perth USAsia Centre