Improving supply chain resilience through preparedness

Andrew Dowse and John Blackburn

Abstract

The COVID-19 pandemic has exposed a lack of national resilience as a result of a collective failure to assess and act on risks in a rapidly changing world. Whilst Australia's economy will remain reliant upon a predominantly global trade model, risks associated with supply chains supporting critical infrastructure need to be assessed and mitigated to acceptable levels. Such mitigations may include a shift in some cases to sovereign solutions, complemented by measures to increase trust in global supply chains. There are implications for Defence supply chains but also potential for a Defence approach to preparedness to contribute to national resilience.

Introduction

Global trade and diverse supply chains are essential for Australia's economic and social well-being. However, over the past decade we have seen our trade and investment profile evolve without any apparent system-wide analysis of resulting risks and vulnerabilities. In pursuit of the lowest cost, we are incurring a very high price in terms of our resilience[1] and sovereignty[2], one which we are yet to fully understand.[3]

Before the onset of COVID-19, many had begun to question the dynamics of Australia's supply chain networks. On the one hand, the world has experienced half a century of uninterrupted integration in trade, affording a myriad of supply chain networks to develop. On the other hand, the market became overly confident in the trade system, having not experienced something similar to the COVID-19 environment. The Coronavirus pandemic has exposed a lack of national resilience as a result of a collective failure to prepare; that is, to assess and act on risks in the face of a rapidly changing world. Disruptions in supply and surge in demand, especially in areas of medical equipment and pharmaceuticals, have coincided with, and to some extent contributed to, a rise in geopolitical tensions.

1 In this context, resilience is the ability of national systems to withstand and recover from adverse events; whereas sovereignty is a nation state's right and power of regulating its internal affairs without foreign interference.

2 Molan, J. (2020) Op-Ed: The importance of a national sovereignty strategy, https://www.defenceconnect.com.au/key-enablers/6004-op-ed-the-importance-of-a-national-sovereignty-strategy addresses the lack of self-sufficiency impacting resilience and thus sovereignty.

3 Blackburn, J. (2020) *Trade without Trust*, submission 42 to the Joint Standing Committee on Trade and Investment Growth Inquiry into Diversifying Australia's Trade and Investment Profile, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Joint_Standing_Committee_on_Trade_and_Investment_Growth/DiversifyingTrade/Submissions.

Australia is particularly vulnerable to trade disruptions in the global marketplace. As an island nation at the end of long global trade routes, we are heavily reliant on just-in-time supply chains, with limited resilience in those chains and low tolerance for loss and disruption. In 2018 alone, there were AUD$317 billion of goods imports and AUD$345 billion of goods exports.[4] While not every element of that trade is critical to our economic and individual well-being, should any significant trade interruption occur, the flow-on effects on the economy, our security and our society would be significant.

In the case of imports, we have incrementally defaulted to the cheapest cost with the result that today we import, for example, 90 percent of our liquid fuels and 90 percent of our medicines, and rely upon foreign-owned/flagged ships for 98 pecent of our trade.[5] The import dependency risks are further compounded by the reluctance of successive Governments to mandate any stockholding levels for these critical imports, unlike many other developed countries.[6]

Australia has, in effect, allowed our resilience to be shaped by the largely foreign-owned market. In this environment, an economic overdependence on any one country, in terms of exports or imports, is a significant risk to our security and sovereignty.[7] If Australia is to maintain an acceptable balance between sovereignty, security, and economic wellbeing, then supply chain risks must be reviewed. The behaviours of a number of countries during the early stages of the pandemic means that our blind faith in the largely foreign-owned market to meet all of our needs in a crisis, without taking precautionary measures such as stockholding or diversification, is foolhardy.

Lack of national resilience is also a concern for our Defence force. Traditional delineations between military and civil affairs are blurred by Defence's reliance on national infrastructure, which utilises foreign supply chains and has significant vulnerabilities. The 2020 Defence Strategic Update acknowledged the risk of vulnerabilities in national infrastructure being exploited by grey zone[8] activities as a precursor to conventional conflict.[9] Military and national security implications of Australia's supply chain vulnerability, therefore, necessitate an integrated approach to risk assessment, leading to calls for a broader approach to national security policy.[10]

---

4 Department of Foreign Affairs and Trade (2019) Composition of Trade Australia 2018, https://www.dfat.gov.au/sites/default/files/cot-2018.pdf.

5 By volume—from Blackburn, J. (2020) *The Implications of the COVID-19 pandemic for Australia's Foreign Affairs, Defence and Trade*, submission 13 to the Joint Standing Committee Foreign Affairs, Defence and Trade inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade.

6 See https://www.dropbox.com/s/8vycz1u54al3uj0/Benchmarking_Australias_Transport_Energy_Policies_Report_December_2014.pdf?dl=0 and https://defense.info/highlight-of-the-week/australias-medical-supply-chain-addressing-strategic-vulnerabilities/.

7 Smith, S. (2001) *Globalization and the governance of space: a critique of Krasner on sovereignty*, International Relations of the Asia-Pacific Vol. 1, No. 2, pp. 199-226 argues the transformative nature of globalisation detracts from sovereignty, however overdependence on any one country represents additional risk.

8 Grey zone activities are operations that may not clearly cross the threshold of war, see Dowse, A. and Bachmann, S. (2019) Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'? https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.

9 Department of Defence (2020) *2020 Defence Strategic Update*, p12, https://www.defence.gov.au/StrategicUpdate-2020/.

10 Dupont, A. (2020) *Coronavirus: Golden opportunity to broaden and strengthen our national security*, The Australian, 13 April 2020, https://www.theaustralian.com.au/commentary/coronavirus-golden-opportunity-to-broaden-and-strengthen-our-national-security/news-story/ae5e6851ebe0cb1a02680d9709884714 and Molan, J. (2020) *Musings on sovereignty*, https://jimmolan.com/article/musings-on-sovereignty/.

Not all supply chains are critical and there are many goods that could be disrupted without significant effect on the nation. This paper will focus on the risks associated with critical supply chains, with two examples to be more closely examined ahead of discussion of national risk mitigations: information technology and fuel. In a future where supply chains may be deliberately disrupted by other nation states as a form of conflict, a discussion of Defence supply chains is central. This paper will start by reviewing the nature of supply chain risks.

Risk Assessment—efficiency versus resilience

There is no doubt that global trade and investment has been advantageous to Australia, with DFAT characterising the benefits of Australia's integration with multiple economies as helping to reduce business transaction costs and providing greater access to global supply chains.[11] This has permitted Australian businesses to gain access to better products and technologies, whilst taking advantage of lower labour rates and economies of scale in production, as well as foreign capital. Additionally, reduction of trade barriers facilitates greater access to export markets and reduces potential for retaliation.[12] There are also comparative advantage arguments to maintaining import levels, especially in a small nation such as Australia where attempting to deliver all products or services would come at an opportunity cost.

The problem of market-driven solutions has been characterised as a loss of resilience through adherence to economic rationalism without sufficient regard for defence and supply chain security.[13] Strengthening resilience is often seen as being at the expense of efficiency, however such a view is based upon the future being 'best case'. Taking a total cost approach would account for the cost of losses associated with disruptive events, potentially justifying more resilient supply solutions that may not appear to be the best value for money. An important lesson is that the cheapest cost comes at a high price in a time of crisis.[14]

To maintain a balance between a lean supply chain and one that accounts for more significant risks is a challenge in an uncertain world. Many businesses seek to identify possible impact events and plan mitigation strategies through scenario planning. Scenario planning in business was pioneered by Royal Dutch/Shell in the 1970s[15] and has been adopted widely, although the variation of methodologies and lack of empirical studies means that there is no agreed consensus on the effects of scenario planning on company performance.[16]

11 Department of Foreign Affairs and Trade (2019) *DFAT 2018–19 Annual Report*, https://www.dfat.gov.au/about-us/publications/corporate/annual-reports/Pages/department-of-foreign-affairs-and-trade-annual-report-2018-19.aspx/annual-report-2018-19/home/section-2/pursue-our-economic-trade-and-investment-agenda-for-opportunity/index.html.

12 Australian Government Productivity Commission (2017) *Rising protectionism: challenges, threats and opportunities for Australia*, https://www.pc.gov.au/research/completed/rising-protectionism/rising-protectionism.pdf discusses the link between tariffs and retaliation although, as evidenced by Chinese actions in 2020, retaliation can also be triggered by matters that are not trade related.

13 Jefferies, W. (2020) *Steel: the future*, Menzies Research Centre, https://www.menziesrc.org/news-feed/steel-the-future.

14 Blackburn, J. (2020) *The Implications of the COVID-19 pandemic for Australia's Foreign Affairs, Defence and Trade*.

15 Wack, P. (1985) *Scenarios: unchartered waters ahead*, Harvard Business Review 63(5), pp 72-89.

16 Phelps, R., Chan, C. and Kapsalis, S. (2001) *Does scenario planning affect performance? Two exploratory studies*, Journal of Business Research, Volume 51, Issue 3, March 2001, Pages 223-232.

The value of scenario planning is challenged by the very uncertainty that it seeks to address. Mintzberg refers to the difficulty of forecasting an uncertain future as the fallacy of prediction.[17] Even when businesses undertake risk planning, those who adopt a probabilistic approach based upon past events will underestimate the strategic impact of future change.[18]

Another pitfall in efforts to develop resilience through identification and mitigation of risks may be the assumption that those risks are independent events. This assumption may lead organisations to prepare for one significant risk, but not multiple significant risks. If the risks are truly independent, this would be a reasonable approach, given the probability of two unlikely events coinciding would be almost negligible.

However, significant events such as a pandemic are likely to generate multiple concurrent risks, such as loss of international transport, increased need for supply, unavailability of workforce, security threats and increased tension with other nation states. In times of state-on-state conflict, such a compounding crisis situation is even more likely as an adversary would pursue multiple concurrent hybrid threats, with emphasis on unpredictability through indirect approaches. Most businesses either do not comprehend the implications of such events or do not believe it is their responsibility to mitigate against them.

Government review of supply chain risks

The Australian Parliament's Joint Standing Committee on Foreign Affairs, Defence and Trade initiated an inquiry in May 2020 to examine the implications of the Coronavirus pandemic. One of the terms of reference was to consider the supply chain integrity of critical enablers of Australian security, including health, economic and transport systems, and defence.[19]

Initial concern about health systems during the pandemic was fuelled by the fact that Australia imports over 90 percent of its pharmaceuticals.[20] An additional concern was for medical equipment such as personal protective equipment and ventilators, as well as supply arrangements for potential vaccines. Whilst the reactive response[21] to address these equipment shortfalls was effective in part, the ability to address medical supply chain risks was less effective as growing concurrent global demand for COVID related medicines and the lack of sovereign manufacturing capability means that a robust medicine supply remains beyond reach.

---

17 Mintzberg, H. (1994) *The Fall and Rise of Strategic Planning*, Harvard Business Review, https://hbr.org/1994/01/the-fall-and-rise-of-strategic-planning.

18 Fuller, T. (2017) *Anxious relationships: the unmarked futures for post-normal scenarios in anticipatory systems*, Technology Forecasting and Social Change 124 pp 41-50 discussed such strategic impacts are more a matter of Knightian uncertainty that probability.

19 Parliament of Australia (2020) *Terms of Reference, Inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/FADTandglobalpandemic/Terms_of_Reference .

20 Coorey, P. (2020) Australia dangerously dependent on medical imports, Financial Review, https://www.afr.com/politics/federal/australia-dangerously-dependent-on-medical-imports-20200217-p541ej.

21 Blackburn, J. (2020) Shortages of personal protective equipment, medical devices, and medicines—what's happening in Australia? https://www.linkedin.com/pulse/shortages-personal-protective-equipment-medical-whats-blackburn-ao/?trackingId=mYWK2ZEpDx47Smg9OL%2Fp7w%3D%3D.

The initial concern surrounding the implications of the COVID-19 pandemic was the pressure placed on the healthcare system. The fact that Australia is a net importer of medical and pharmaceutical goods made it particularly vulnerable to shortages in the medical supply chain. The COVID-19 pandemic has brought forth three major problems concerning supply chain risks of medical equipment. Since the beginning of the pandemic, there has been a surge in demand from healthcare systems around the world. Also, the disruption to inputs to supply chains has arisen from public health measures such as lockdowns, thus constraining supply. Finally, the health emergency has prompted over 50 governments, including Australia, to place restrictions on exports of medical supplies and equipment.

Several submissions to the Inquiry drew conclusions about supply chain vulnerabilities in the context of growing geopolitical tension. Dupont[22] notes the growing advocacy for national resilience and self-sufficiency, especially with vulnerabilities of imports of critical products from China. He promotes an astute and moderate approach to decoupling from risky relationships while retaining global trade—essentially finding the right balance between risk reduction and cost reduction. Coercion and other grey zone acts by nation states have been evident during the pandemic and will increasingly create supply chain disruption.[23] In the case of critical infrastructure services, supply chain risks should be reviewed, and mitigations implemented accordingly.

A further risk for our national resilience is where the quality or integrity of a supply chain creates an impact, either deliberately or inadvertently. The integrity threat is a growing concern, especially for information technologies.

ICT supply chains

Given the increasing reliance of our economy, security and society on connected information systems, Information and Communications Technology (ICT) supply chains and cyber security are important considerations for national resilience. With the connectivity and cyber-physical integration of the fourth industrial revolution, control and disruption of information systems will increasingly be a means of achieving an advantage in global competition and conflict.

Although ICT is fundamental to our economy and daily lives, the understanding of our supply chain dependencies and risks in this domain is evolving at a slower pace than the growth of the threats.[24] The risk of cyber attacks is increasing, as is the number of major attacks.[25] The Australian Signals Directorate (ASD) assesses that malicious cyber

22 Dupont, A. (2020) *Submission 6 to JSC FADT inquiry into the implications of COVID-19*, Cognoscenti Group, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/FADTandglobalpandemic/Submissions.

23 Dowse, A. and Bachmann, S. (2020) Submission 7 to JSC FADT inquiry into the implications of COVID-19, Cognoscenti Group, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/FADTandglobalpandemic/Submissions.

24 Blackburn, J. and Waters, G. (2011) *Optimising Australia's Response to the Cyber Security Challenge*, Kokoda Foundation Paper #14, https://www.dropbox.com/s/q1fjmzrf9doxxit/Kokoda%20Cyber%20Report%20.pdf?dl=0.

25 European Court of Auditors (2019) *Challenges to effective EU cybersecurity policy*, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

attacks against Australian interests are increasing in frequency, scale, sophistication and severity[26], noting that the vast majority is cyber crime with an emphasis on quantity over quality.[27]

Although spending on cyber security is growing[28], the cost of cyber crime in Australia is increasing at a greater rate.[29] More concerning, however, is the prospect of a surge in attacks, especially in the context of broader conflict and in the knowledge that nation states may be stockpiling exploits for zero-day vulnerabilities.[30] Given this potential, the total cost of cyber risks need to be considered, not just the cost of previous events.

As technologies have evolved, so too must mitigations to deal with more pervasive threats. Strengthening traditional perimeter defences to secure cyber vulnerabilities may seem appealing, but will not suffice. Increased mobility and connectivity of modern ICT necessitate a different approach. Additionally, our nation's critical infrastructure and defence systems utilise technologies that may be untrusted.[31] The exploitation of ICT through external connectivity is not the only risk; often it is the integrity of the ICT itself.

With an estimated 15% of US military parts being counterfeit[32], there is potential for malicious and catastrophic consequences if such equipment is used. The same potential exists for ICT. Quality deficiencies or deliberate exploits may be introduced within a global supply chain. The tendency to solicit for the best value for money for ICT products through an open process especially raises this risk through grey market equipment.[33] Greater controls over the source of ICT is needed to mitigate the risk. Such controls have been evident in Government action regarding the sourcing of 5G technologies.

Encouraging the growth of Australia's IT industry would improve security through sovereign technology control within our supply chains, while also delivering economic value. However, aspirations realistically may need to be limited to niche capabilities and technologies that support critical functions, given the scale of resources needed to develop and maintain quality systems. Australia's IT will need to remain dependent on assured global supply chains.

Australia's future IT supply chains should be assured through a combination of trusted global partners together with a concentration of sovereign IT expertise in capabilities that provide security in an untrusted environment. This approach is supported by the

26 ACSC (2017) *ACSC 2017 Threat Report*, https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf.

27 ASD (2019) *Annual Report 2018/19*, https://www.asd.gov.au/publications/annual-report-2018-19.

28 AustCyber (2019) *Australia's Cyber Security Sector Competitiveness Plan: 2019 Update*, https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

29 Tonkin, C. (2019) *Australian cybercrime surge costs millions*, ACS Information Age, https://ia.acs.org.au/article/2019/australian-cybercrime-surge-costs-millions.html.

30 Ablon, L. and Bogart, A. (2017) *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, RAND Corporation, http://www.rand.org/pubs/research_reports/RR1751.html.

31 This is not to say that they are malicious, but that inadequate attention has been invested into ascribing trust.

32 Wagner, P. (2015) *Combating Counterfeit Components in the DoD Supply Chain*, DSIAC Journal, Spring 2015, Vol 2 No 2.

33 Annu-Essuman, K. (2014) *An Analysis on the Regulation of Grey Market Cyber Materials*, Cornell International Affairs Review 8:1, http://www.inquiriesjournal.com/articles/1193/an-analysis-on-the-regulation-of-grey-market-cyber-materials.

Government's cyber security strategy[34], which highlights the need to engage with like-minded nations on the security of critical technologies; higher expectations of businesses to protect assets, especially in critical infrastructure; and the strengthening of Government defensive cyber capability. This approach needs to consider data and support services, not only supply of products, especially after instances of interruption to services such as call centres caused by shutdowns during the pandemic.[35] The impact of loss of these services to customers of telecommunications companies and banks is another example of the price that comes with a low cost.

Fuel supply chain risks

Fuel is often discussed as a key national supply risk, and with good reason. As at May 2020, Australia had 59 days of net oil stockholdings, by far the lowest, and only non-compliant, of the International Energy Agency (IEA) member countries.[36] The Government view is that fuel reserves should include stock "on water", despite this being contrary to the IEA guidance, outside of our direct control and still representing less than our IEA membership obligation of 90 days.[37]

The problem is that the net oil stockholdings figure does not clearly show what our useable fuel stocks are in Australia: the two are often confused by commentators. Australia cannot consume "net oil stockholdings": it is an accounting figure. Australians, including the Australian Defence Force (ADF), can only consume actual stocks of fuels held in Australia by specific fuel type, and only if the fuel can be delivered to facilities when and where they are needed. The actual useable fuel stockholdings as at May 2020 were: 18 days of diesel and 31 days of aviation jet fuel.[38] The aviation jet fuel stocks at that time were higher than usual, possibly due to the lower consumption of aviation fuels resulting from COVID-19 travel restrictions. None of these stocks in Australia is Government owned and there were no mandated minimum stockholding levels. In other words, it was left to the largely foreign owned market to decide what stock levels are maintained, until the Government announcement in September 2020 that introduced mandatory stock levels.

Other significant issues with respect to supply of fuels include vulnerabilities of supply routes for liquid fuel transit, as well as their carriage exclusively on foreign flagged ships; foreign ownership of the remaining major refineries in Australia; and the lack of government policy to ensure Australia's refineries remain operational. Additionally, an

34 Commonwealth of Australia (2020) *Australia's Cyber Security Strategy 2020*, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

35 Fernyhough, J. (2020) *Telcos rush to fill gap as Indian call centres close*, Australian Financial Review, https://www.afr.com/companies/telecommunications/telcos-rush-to-fill-gap-as-indian-call-centres-close-20200325-p54dqq.

36 Ton, W., Lane, J. and Trute, P. (2019) *Does Australia have close to 90 days oil reserves*? https://factcheck.aap.com.au/claims/does-australia-have-close-to-90-days-of-oil-reserves and IEA (2020) *Oil Stocks of IEA Countries*, https://www.iea.org/articles/oil-stocks-of-iea-countries.

37 Tillett, A. (2020) *Australia buys two days of cheap fuel*, AFR 22nd April 2020, https://www.afr.com/politics/federal/australia-buys-two-days-of-cheap-fuel-20200422-p54m6h.

38 Department of Industry, Science, Energy and Resources (2020) *Australian Petroleum Statistics Issue 286*, p66 https://www.energy.gov.au/sites/default/files/Australian%20Petroleum%20Statistics%20-%20Issue%20286%20May%202020.pdf noting that these are national figures, not reflecting Defence holdings of Defence-specific fuel types.

April 2019 Government report highlighted that "there is no overarching understanding of the whole liquid fuel market in Australia and how different parts interact with each other."[39]

Existing fuel distribution chains within and around Australia are designed for just in time, "business as usual" consumption, incapable of dealing with unexpected surges.[40] Australia cannot therefore have confidence that just-in-time commercial supply chains will provide sufficient fuels to our Defence forces, and our society at large, in a time of escalated operations.

Australia's acceptance of fuel supply risk is based on a flawed and naïve assumption exemplified by this quote in an article in *The Australian*: "The Energy Department said Australia's low supplies were not a serious concern as there had never been a serious interruption to Australia's supply."[41] Given the chaotic, cascading, effects of the pandemic on our society, it is worth reassessing such logic. Indeed, there is a broader lesson that we should not prepare for strategic surprises in an uncertain future by considering only the prevalence of events in the past.

There is no Government owned strategic oil or fuel reserves in Australia, no Government control over the importation of 90 percent of our oil and fuel requirements, and no contingency plan should a major interruption of supply occur. Cognisant of these deficiencies, the March 2018 the Australian Parliament's Joint Parliamentary Committee (JPC) on Intelligence and Security recommended that the Government review and develop measures to ensure that Australia has a continuous supply of fuel to meet its national security priorities.[42] Despite the committee advocating for the review to take place within six months, it is yet to be publicly released. Australia is unprepared and would not be resilient in the event of a major fuel supply chain interruption.

The initiative in April 2020 to utilise the US Strategic Fuel Reserve was claimed by the Australian Government to contribute to IEA stockpiling obligations[43], however the real contribution of offshore stock to fuel security is debatable. The September 2020 announcement of measures associated with onshore storage and local refinery capability[44] represents a far more tangible contribution and is an excellent first step. Unfortunately the

39 Department of the Environment and Energy (2019) Liquid Fuel Security Review, p20, https://www.environment.gov.au/system/files/consultations/7cf6f8e2-fef0-479e-b2dd-3c1d87efb637/files/liquid-fuel-security-review-interim-report.pdf.

40 Australia witnessed how domestic supply chains could not cope with the irrational surge in demand for toilet paper during the early phases of the pandemic and disruption to fuel supply could lead to similar irrational surges for fuel. Similar challenges were evident in aviation fuel distribution chains when search operations based in Western Australia for the Malaysian Airlines Flight 370 caused significant stress in the State's fuel distribution system.

41 Riordan, P. (2019) *Red light flashing over fuel security*, The Australian, 6 Jan 2019, https://www.theaustralian.com.au/nation/politics/red-light-flashing-over-fuel-security/news-story/4d5101e1585ddc95017beb946d184f9f.

42 Australian Parliament (2018) *Advisory report on the Security of Critical Infrastructure Bill 2017*, Parliamentary Joint Committee on Intelligence and Security, recommendation 3.6, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CriticalInfrastructure/Report.

43 Taylor, A. (2020) *Australia to boost fuel security and establish national oil reserve*, https://www.minister.industry.gov.au/ministers/taylor/media-releases/australia-boost-fuel-security-and-establish-national-oil-reserve.

44 Taylor, A. (2020) *Boosting Australia's fuel security*, https://www.minister.industry.gov.au/ministers/taylor/media-releases/boosting-australias-fuel-security.

announcement by BP on 30 October 2020 that it intends to close their Refinery in Perth[45], combined with the announced review by both Viva and Ampol regarding the potential to close their refineries, means that the Government's initiative may be too little, too late.

Loss of refining capability in Australia represents a significant risk, and stockholding alone will not address the JPC recommendation that the Government review and develop measures to ensure that Australia has a *continuous supply* of fuel to meet its national security priorities. Increasing domestic stocks of liquid fuels is an important measure but will need to be balanced with demand-side efforts. If we purely mandate stocks without thinking about how to curb demand for imported fuels by increasing local transport energy options, the current strategy won't be resilient enough to withstand a range of global crises in the future.

Improving national resilience

Resilience is defined as the ability of a system that is exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner.[46] Australia's view of national resilience has a long and extensive connection with our ability to withstand natural disasters, however, this understanding can also be extended to other hazards and threats. The Critical Infrastructure Resilience Strategy[47], published in 2015, emphasises the need to maintain continuity in the face of acts or events that might otherwise significantly impact the social or economic wellbeing of the nation. It also highlights Australia's ability to conduct defence and ensure national security as a foundational element of resilience.

However, resilience is but a characteristic or attribute of our society, individually and collectively. We cannot be truly resilient unless we are prepared. Australia has reacted very well to the pandemic, but arguably was not adequately prepared for this or a range of other significant risks that could eventuate.[48]

Australia's recent efforts towards building national resilience have been undertaken on two lines of effort. The National Resilience Taskforce, established in 2018, developed a risk framework[49] as well as an analysis of causes and cascading effects of disasters.[50] Although its risk framework approach was cogent, the taskforce's work was limited to dealing only with natural disasters. This is a significant limitation. The taskforce came

45 Toscano, N. (2020) *BP to shut Australian oil refinery, leaving just three in the country*, SMH 30 October 2020, https://www.smh.com.au/business/companies/bp-to-shut-australian-oil-refinery-leaving-just-three-in-the-country-20201030-p56a5f.html.

46 National resilience taskforce (2018) *Profiling Australia's vulnerability*, https://www.aidr.org.au/media/6682/national-resilience-taskforce-profiling-australias-vulnerability.pdf.

47 Commonwealth of Australia (2015) *Critical Infrastructure Resilience Strategy Plan*, https://cicentre.gov.au/document/P50S021.

48 Institute for Integrated Economic Research (2020) *Australia's Medical Supply Chain: Addressing Strategic Vulnerabilities*, https://defense.info/highlight-of-the-week/australias-medical-supply-chain-addressing-strategic-vulnerabilities/.

49 Commonwealth of Australia (2018) National Disaster Risk Reduction Framework, https://www.homeaffairs.gov.au/emergency/files/national-disaster-risk-reduction-framework.pdf.

50 National Resilience Taskforce (2018) op cit.

under extensive criticism following the 2019 bushfires, for failing to proceed with timely implementation.[51]

Risks associated with other events such as deliberate acts were addressed by the Critical Infrastructure Centre, also part of the Australian Department of Home Affairs, and its Critical Infrastructure Resilience Strategy released in 2015. This strategy is directed towards four outcomes of partnerships, risk management, strategic management, and organisational resilience.[52] Perceptions that this strategy is not doing enough for national resilience has led to action from Home Affairs. A 2020 consultation paper has identified the need for stronger regulation, improved articulation of responsibilities and expectations, and greater cyber protection.[53] Whereas the consultation paper is primarily concerned with cyber threats, it includes an expectation that broader risks to supply chains will be addressed through a risk-based approach.

Such a regulatory validation of critical infrastructure providers' risk management should provide a greater sense of comfort that our supply chains will be more resilient. Decisions about risks cannot be left to the market alone, as has been the case in the past. Service providers might downplay the likelihood of adverse events to maximise short term profits, but additionally may be more willing to accept risk of adverse events.[54] Accordingly, risk management needs to include a supply chain illumination process, in which a top down process identifies critical components within subordinate supply chains and considers mitigations. In implementing those mitigations, we should be prepared to accept that avoiding future costs will come with an upfront cost.

With the interdependent nature of our nation's systems and the threats against them, in one way it may be advantageous for an integrated approach that addresses supply chain risks for a wide range of adverse events, including deliberate acts and disasters. After all, the Coronavirus pandemic has demonstrated that the cascading and compounding effect of such events may be challenging for traditional approaches to risk management.

Mitigating national supply chain risks

National supply chain risks are primarily concerned with assured availability. The threat to that availability could be due to an issue at the source of supply, whether domestic or overseas. These issues could be caused by the cascading effects of a natural disaster, pandemic, or conflict. Global supply chains can also be disrupted due to transport disruption, or because the supplier holds back supply (due to competing demands, political motivation, or during conflict).

One solution to such vulnerabilities is the establishment of appropriate sovereign capabilities and related supply chains supporting critical infrastructure services.

51 Fernyhough, J. (2020) *Government buried climate risk action plan*, Financial Review https://www.afr.com/politics/federal/government-buried-climate-risk-action-plan-20200110-p53qeg.

52 Commonwealth of Australia (2015) op cit.

53 Department of Home Affairs (2020) *Protecting Critical Infrastructure and Systems of National Significance*, https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf.

54 In many scenarios, adverse events such as loss of supply may impact the customer far more than the supplier.

A methodical review of the risks associated with critical infrastructure services[55] could identify those elements of the supply chains for which a sovereign solution is justified, affordable, and viable. Importantly, the value for money consideration of such solutions should take into account potential loss reduction—that is, to price in a crisis.

Australia also needs to consider the redesign of critical components of our industry base and supply chains under a 'Smart Sovereignty' model.[56] Such a model should not be construed as socialism or nationalisation of whole sectors of the economy. Smart Sovereignty infers not only a degree of Australian based manufacturing capability and associated domestic supply chains, but the appropriate research and development facilities and a skilled, experienced workforce.

Determining where and how much sovereign capability that we must have, to be resilient as a nation, will be a complex task. There will be limits to sovereign industry levels, due to Australia's finite resources, the value of efficiencies gained through global supply chains and the negative consequences of mercantilism. Therefore, the essential complement to Smart Sovereignty will be the establishment of "Trusted Supply Chains", in cases of dependence on global trade imports for critical systems. For these imports, Australia must have diverse and transparent supply chains and have the ability to verify them.[57] In addition to supply chain diversification, interdependent supply partnerships with select nations could be an important contributor to national resilience.

Defence supply chain resilience

Given their centrality to national security, Defence's supply chains deserve specific attention. Defence's primary concern with supply chain risks has been the availability of warfighting equipment, including parts, as well as consumables such as fuel. With the shift to outsourcing over the past three decades, these risks also include the availability and effectiveness of external support services and infrastructure (including contracted maintenance, power supplies and ICT services). The supply chain risks include fitness-for-purpose, not just the availability of supply items. Additionally, many items have short in-use or shelf life, for which Defence must balance the efficacy of just-in-time supply chains with large-scale stockholdings.

Up until the release of the 2020 Defence Strategic Update[58], the Defence strategy on supply chain security varied little. The 1987 White Paper noted the centrality of the US alliance for timely supply of military equipment and ammunition, reducing the need for stockpiling.[59] Having said that, the 1987 White Paper also notes the possibility that this supply could be disrupted, thus highlighting the need for arrangements to reduce temporal disruptions by developing and retaining sovereign maintenance capability in industry, stocks of consumables, and technology capability expertise in certain areas.

55 As advocated by Home Affairs in *Protecting Critical Infrastructure and Systems of National Significance.*

56 Blackburn, J. (2020) op cit.

57 Ibid.

58 Department of Defence (2020) op cit.

59 Department of Defence (1987) *The Defence of Australia 1987*, https://www.defence.gov.au/Publications/wpaper1987.pdf.

Similarly, the 2000 White Paper noted the need for in-country support for repair, maintenance, modification, and provisioning, as well as stockpiling of high cost foreign-sourced provisions such as guided weapons.[60]

The 2009 White Paper softened its guidance on critical provisions, accepting risks dependent on global supply chains and noting that a stable Southeast Asia can mitigate threats to fuel supply sea lines of communication.[61] Citing the Mortimer Review, it called out the significant waste present in logistics and directed that greater efficiencies be achieved in inventory management and supply chain arrangements. Priority Industry Capabilities (PICs) were introduced as a mechanism to retain sovereign capability in certain areas.[62] Subsequently, the 2013 White Paper was largely silent on supply chain resilience, simply accepting risks of dependence on the global supply chain and noting that any threat to such arrangements would invoke support from the US.[63]

The 2016 White Paper also played down concerns with supply chains, other than highlighting the importance of a national support base to Australia's resilience.[64] The only obvious initiative identified against this requirement was the classification of defence industry as a fundamental input to capability and the promise of a change to the PIC framework to develop sovereign industry capabilities.[65]

The 2018 Defence Industry Capability Plan provides a fuller articulation of the roadmap to build the national defence industry base.[66] It focuses efforts on the ten sovereign industry capability priorities derived from the earlier PICs, designed to contribute to the most critical Australian Defence Force requirements. Although primarily concerned with supporting the ADF, there is also a strong emphasis on delivering economic outcomes in delivering capability within global supply chains.

The Defence Industrial Capability Plan is primarily designed to deliver strategic resilience against longer-term shifts in technology availability by building a national industry in key areas. It is not designed to deliver resilience to crises that may impact the ADF's ability to surge and sustain operations in the face of short-term disruptions to supply. The priorities for munitions manufacture and aerospace deeper level maintenance could provide some mitigation to temporal risks. Nevertheless, the main focus is on developing defence industry to build military systems, which is driven more by longer term objectives and economic benefits than the need for resilience.

60 Department of Defence (2000) *Defence 2000—Our Future Defence Force*, https://www.defence.gov.au/publications/wpaper2000.pdf.

61 Department of Defence (2009) *Defending Australia in the Asia-Pacific Century: Force 2030*, https://www.defence.gov.au/whitepaper/2009/docs/defence_white_paper_2009.pdf.

62 Purnell, L. and Thomson, M. (2009) *How much information is enough?: The disclosure of defence capability planning information*, https://www.jstor.org/stable/resrep04180.11?seq=5#metadata_info_tab_contents pp 63-64 asserts that the PICs fell short of providing guidance to Australian industry.

63 Department of Defence (2013) *Defence White Paper 2013*, https://www.defence.gov.au/whitepaper/2013/docs/WP_2013_web.pdf.

64 Department of Defence (2016) 2016 Defence White Paper, https://www.defence.gov.au/Whitepaper/Docs/2016-Defence-White-Paper.pdf.

65 Introduced in the accompanying 2016 Defence Industry Policy Statement https://www.defence.gov.au/Whitepaper/Docs/2016-Defence-Industry-Policy-Statement.pdf.

66 Department of Defence (2018) *Defence Industrial Capability Plan*, https://www.defence.gov.au/spi/industry/capabilityplan/Docs/DefenceIndustrialCapabilityPlan-web.pdf.

Another concern with the Defence Industrial Capability Plan is that it does not build upon any national industrial plan, or at least provide the broader national industry context. There are two reasons it should do so. Firstly, Defence is reliant upon not only a robust defence industry sector but also a robust broader industry capability across areas such as manufacturing, engineering, and information technology. Whilst this may seem like the 'tail wagging the dog', a capable national industry base is critical to the sustainability of the defence sector, including the maintenance of skills. In many cases, it is also critical to the security/availability of defence capability, given defence's reliance on national capabilities such as in transport, energy and telecommunications. The second reason it should do so is that, with the increasing threat of hybrid warfare[67], the resilience of the national industry is something that Defence will need to address in a conflict.

Despite the intent of PICs and sovereign industry priorities, the level of domestic expenditure in defence acquisition and sustainment has not varied since their introduction.[68] The Defence Industrial Capability Plan specifies criteria behind the sovereign industry capabilities, including independence of action and assurance of supply.[69] Yet in practice, these have not been evident. Marcus Hellyer of the Australian Strategic Policy Institute (ASPI) highlights the risk that even when capabilities are built in Australia, they can be impacted by disruptions in foreign sourced supplies, as was the case with the Hawkei protected vehicle project.[70] He also highlights the inadequacy of the stock of guided missiles and fuel, noting that these effectively limit conventional conflict options to days.[71]

Defence recognises the risk of such supply chain deficiencies and has even explicitly accepted such risks in past White Papers—in the same way that a homeowner might decide not to insure against certain risks, despite the significance of their impact if they are realised. However, recent deterioration of the strategic environment led to a shift in Defence's position with the 2020 Defence Strategic Update, which stressed the need for more secure supply chains.[72] The update includes the need to address vulnerabilities in supply chains associated with Internet access (s1.11), fuel and ammunition stocks (s1.13, s3.30), critical supplies needed to maintain operations (s1.16), the need for assurance of global supply chains (2.26) and the ability to operate at a high intensity (s3.30). Importantly it also discusses the importance of depth and flexibility of supply, with increased trust in global supply arrangements complementing domestic industry initiatives.[73]

The Defence Strategic Update was already underway before the pandemic, but has been skilfully adjusted to recognise new realities. Its recognition of the deteriorating strategic environment together with realisation of supply chain vulnerabilities has led to a justified call for action. This represents a departure from an ongoing acceptance of

67 Hybrid warfare relates to the application of multiple, diverse tactics simultaneously against an adversary, see Dowse, A. and Bachmann, S. (2019) *op cit*.

68 Hellyer, M. (2020) *Supply chain security: lessons from Australia's defence industry*, ASPI https://www.aspistrategist.org.au/supply-chain-security-lessons-from-australias-defence-industry/.

69 Department of Defence (2018) *Defence Industrial Capability Plan*, s2.7

70 Hellyer, M (2020) op cit.

71 ibid

72 Department of Defence (2020) op cit.

73 ibid

those vulnerabilities, consistent with the appreciation that strategic warning times are no longer reliable. However, it remains to be seen whether this will lead to any action to address supply chain vulnerabilities. After all, Defence is limited in its ability to take substantial action without an integrated national effort.

Implications for Defence

The Defence Strategic Update provides a sobering analysis of the recent changes in our strategic environment, including great power competition, challenges to the stability of the rules-based global order, and the emergence of new, complex non-geographic threats.[74] This follows the Australian Defence Minister's acknowledgement of the emergence of grey zone and hybrid threats.[75]

Such future threats may employ an indirect approach[76] to target the nation, rather than the military. Together with interdependence on global supply chains and national infrastructure, this indirect threat means that Defence needs to consider a broader view of its supply chain vulnerabilities, as well as the nation's vulnerabilities that Defence may be called upon to defend.

This paper has highlighted two areas of supply chain risk, both of which are highly relevant to Defence. Defence fuel supply chain resilience has been recognised with the initiation of an associated remediation program.[77] Notwithstanding, Defence's fuel risks will continue to be exacerbated by the lack of national fuel resilience and the challenge of having special fuel needs.

The increasing dominance of the information domain means that ICT is a critical source of risk to Defence. Of notable importance is artificial intelligence (AI) which, given Australia lacks national policy on its development or use, will likely take the well-trodden path of the market taking the most cost-effective approach. A dependence on overseas development of AI will represent significant risk, given the central place that AI will have in cyber-physical systems. AI systems will create a significant challenge in the ability to establish trust through transparency and verification, as such systems by design do not act in a predictable manner. This will place even greater criticality on risk assessment of AI systems, with a greater implication therefore for sovereign and trusted supply chains.

Defence policy is about identifying priorities and, in this regard, the Sovereign Industry Capability Priorities (SICP) are of pivotal importance to the development of Australia's defence sector. A similar approach could also be taken to development of sovereign industries for supply chains supporting nationally significant capabilities.

Defence needs to progress supply chain mitigations associated with operational vulnerabilities, not just long-term acquisition priorities. The SICP do not provide a path to

74 Department of Defence (2020) op cit, p11.

75 Reynolds, L. (2019) *ASPI International Conference: War in 2025*, https://www.minister.defence.gov.au/minister/lreynolds/speeches/aspi-international-conference-war-2025.

76 Consistent with the indirect approach concept described by Liddell Hart, B. (1967) *Strategy*, Second Revised Edition. New York, NY: Fredrick A. Praeger Publishers.

77 Levick, E. (2018) *Defence Fuel Transformation Program expanded*, https://www.australiandefence.com.au/estate/defence-fuel-transformation-program-expanded.

achieve the security of supply chains that the Government seeks in the Defence Strategic Update 2020. While one option may be to expand the SICP, this may complicate their acquisition focus and long-term deliberate implementation.[78] Ideally, what is needed is the incorporation of new initiatives to complement the SICPs and secure Defence's supply chains.

Such supply chain mitigations may be reliant upon national resilience and Defence cannot itself lead a program that addresses our national limitations. It can, however, enable and support such a process given the extensive expertise and experience in risk analysis, scenario war gaming, preparedness, exercising, and training. Such expertise may assist both the public and the private sector to understand the risks, perhaps through the conduct of informing workshops. Defence can also set an example for national resilience by reviewing its supply chain risks and implementing associated policies.

Defence should offer to take a supporting and enabling role in reviewing national resilience and supply chain risks, as well as associated mitigations and responses, at the least. This is consistent with the Government's expectation of the ADF to shape, deter, and respond to threats against the nation's interests.[79] It would also reflect the expertise that ADF personnel has in appreciating and planning to defeat such threats.

In responding to the pandemic, Australians have seen the value of highly trained, professional and disciplined ADF teams in supporting our community. However, Defence is capable of much more than guarding hotels, carrying luggage, supporting police and conducting border checks. It knows how to prepare for and operate effectively in a crisis; it is resilient because it is prepared. Defence, partnered with other "operational" Departments such as Home Affairs, should help Federal and State Governments and Agencies to be better prepared for the crises Australia will inevitably face in the forthcoming decades. Continuing to be surprised and taking a reactive approach to adverse events is not good enough.

If Australia is to improve national resilience, our lack of preparedness must be remedied. In this endeavour, Defence concepts and systems could be of assistance. For example, the initial focus of the RAAF's Plan Jericho to build a 5th Generation Force was to target vastly improved shared awareness and the ability to operate as an integrated team.[80] Awareness in the sense of shared knowledge of a situation, both current and emerging, is based on a comprehensive risk analysis with recognition of implicit assumptions. The theme of the integrated team is often considered as the willingness to act together for the common good to achieve shared goals, balancing competition and collaboration. This is in effect what successful joint military operations are about.

Utilising the principles of shared awareness and the ability to operate as an integrated team, Defence prepares for operations under a well-established preparedness system. The ADF does not perform as professionally as it does because it is just good at reacting. The preparation of the ADF in all aspects, the analysis of the risks, an understanding of vulnerabilities, the development of operating concepts and plans, and then the

78 For example, the third of ten implementation plans was issued two years after issue of the Defence Industrial Capability Plan.

79 Department of Defence (2020) op cit, p4.

80 AIRMSHL G. Brown Speech—https://australianaviation.com.au/2015/02/caf-launches-plan-jericho/.

comprehensive training and exercising of the force, is what produces excellent operational results. This approach, adapted for wider use across our nation, is what could enable our nation to be better prepared for the range of risks we face in forthcoming decades. Supply chain resilience is but one component of those risks that must be addressed.

Conclusions

Australia should not try to replicate the previous environment after COVID-19. The recovery phase is an opportunity to establish greater resilience in our supply chain arrangements against disruptive events. To do so means that resilience needs to be considered in the broader context of potentially adverse situations, including conflict and the prospect of cascading and compounding events.

Risk management is a critical part of the shift to more secure supply chains, as has been signalled in the recent Home Affairs Critical Infrastructure consultation paper and Defence Strategic Update. For those initiatives to truly result in more secure supply chains will depend on three key factors. Firstly, there needs to be a balance of cost reduction with risk reduction, in which a total cost approach prices in plausible adverse events. Secondly, risk acceptance should be aligned with who is impacted by the risk, not just the service provider. Thirdly, a broad view of plausible risks needs to be taken, including for critical infrastructure to look beyond cyber threats.

There is no prospect that all critical supply chains will be Australian owned or controlled. Consideration of Australia's strengths, costs and opportunities together with a robust risk management process should enable a systematic approach to redesigning supply chains. A Smart Sovereignty model will ensure the industry and skilling inputs to those supply chains are developed. The essential complement to Smart Sovereignty will be the establishment of trusted supply chains, with a foundation of strong relationships, verification processes, diversification and contingencies. Such arrangements should be supported by a national preparedness strategy and plan, managed by an integrated team.

Although improving national supply chain resilience is necessarily a Whole-of-Government endeavour, Defence is exposed to risks associated with its supply chain vulnerabilities as well as indirectly from supply chains supporting national infrastructure. Regardless of whether the result of disaster events or a deliberate attack by a nation state, Defence has a significant stake in our national supply chain resilience. Additionally, Defence has the skills and a preparedness regime that could be utilised for wider use across the nation to enable us to be far better prepared for the range of risks we face in forthcoming decades.

The Critical Infrastructure Consultation paper and the Defence Strategic Update provide a positive shift towards an appreciation of supply chain risks and the prospect that these may be mitigated within a total cost approach to enhance national resilience. With experience of supply chain management, preparedness and the planning associated with potential conflict, Defence should take a key role in enabling and supporting national efforts.

The pandemic has been a wake-up call for Australia. We must learn lessons in the broader context of an uncertain future and invest effort to secure our supply chains. Although integration with global supply chains has been of economic benefit, we need to be smarter about our dependencies in the future and not leave Australia's national resilience to the market.

Andrew Dowse AO PhD is the Director of Defence Research as well as Research Leader in Information Warfare at Edith Cowan University.

John Blackburn AO is a consultant in the field of Defence and National Security. He is the Board Chair of the Institute for Integrated Economic Research—Australia and a Fellow of the Institute for Regional Security.