Inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade

Submission to Joint Standing Committee FADT

By A Dowse and S Dov Bachmann

We would like to thank the Joint Standing Committee for the opportunity to contribute to the Inquiry into the implications of the COVID-19 pandemic for Australia's foreign affairs, defence and trade. We believe our input is relevant to the terms of reference, specifically the implications for policy, threats to global rules-based order, supply chain assurance underlying Australia's security, and the need for measures to enhance national resilience and objectives.

Synopsis

The obvious focus for Government into implications of COVID-19 is on those consequences that arise directly from the pandemic and the associated restrictions to protect our citizens. However, there are secondary consequences in terms of opportunistic activities especially by State actors to further their interests. These indirect consequences should be the main focus for the Joint Standing Committee's consideration of COVID-19 implications, and are the basis of our input to the inquiry.

Background

In 2019, some six months before the emergence of COVID-19, Australia's Defence Minister and Chief of Defence each raised concerns about the threats to our national interests from nations pursuing strategic ends in the **grey zone**, below the threshold of traditional armed conflict[i]. While the intent of pursuing strategic ends without resorting to violent conflict is not new and indeed entirely consistent with the Clausewitzian view of war, our Defence leadership drew attention to the grey zone threat because of the increasing ease with which effects can be achieved through information technology.

Related to this concept of the grey zone is **hybrid warfare**, so called because it involves a combination of unconventional methods within a multi-domain approach[ii]. Hybrid warfare includes a variety of tools, such as cyber and political warfare, that may be coordinated to best effect and may be difficult to attribute or defend. We contend that there is no silver bullet against grey zone and hybrid threats, but the variety and coordination of such threats need to be met by a variety and coordination of defence mechanisms[iii].

Hybrid threats are multimodal, low intensity, kinetic as well as non-kinetic threats to international peace and security. Examples of hybrid threats include asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction. Cyber warfare is an example of the use

of new technologies within the scope of hybrid threats. The combination of new technology and its availability to a multitude of actors make cyber-supported or cyber-led hybrid threats so potent. Russia has been one of the most prolific users of cyber warfare capabilities. In 2007, Russia attempted to disrupt Estonia's Internet infrastructure as retribution for the country's removal of a WWII Soviet War Memorial from the centre of Tallinn. Russia also augmented its conventional military campaign in Georgia with cyber capabilities, which severely hampered the functioning of government and business websites. In the present conflict in Eastern Ukraine, Russia has effectively used the information sphere as an integral tool in its hybrid war against the people of Ukraine.[iv]

The CCP is using its own brand of hybrid warfare in the form of "unrestricted warfare" which takes place in multiple domains including environmental warfare, financial warfare, trade warfare, cultural warfare, and legal warfare.[v] China achieves its foreign policy and military goals with evolving strategies, including propaganda at horizontal and vertical levels. It emphasizes "influence operations," which are materialized in the "three warfares" (san zhong zhanfa) that comprise: 1) *Public Opinion*, which intends to project a positive image of China domestically and abroad; 2) *Psychological Warfare*, which seeks to undermine an enemy combat operations by deterring and demoralizing enemy military personnel and supporting civilian populations; and 3) *Legal Warfare*, which uses national and international law to support Chinese interests.[vi]

Pandemic Implications

So how is this relevant to the implications of the pandemic? What we have seen during the COVID-19 pandemic is a realisation of the concerns about our (and our allies') vulnerability to these grey zone threats, with evidence that State actors are using the disruption to further their objectives through such activities; and recognition that there are vulnerabilities to such threats that could be exploited further.

One of the most significant concerns has been the impact of **disinformation** activities on our ability to deal with the pandemic, as well as to maintain stability and social cohesion. The significance of the disinformation problem is such that it has been widely referred to as an 'infodemic'. Much of this infodemic problem is related to societal trends in information, including the increasing dependence of citizens on social media as a news source, the ability for unsubstantiated information to become viral, and mistrust in traditional institutions and Government. These trends have led to widespread acceptance of clearly false information about potential cures and causes of COVID-19[vii].

Social media has been manipulated by nation states to spread disinformation, such as in relation to the origin of COVID-19. Whilst we have seen some action to address the problem of fake accounts[viii] and false information, there is a lack of consensus on the role of the providers or whether their efforts will be effective or introduce other problems. Whether disinformation is facilitated by nation state efforts or through the very nature of social media, the Committee might consider the need for measures to reduce the impact on the population. Such considerations could be informed by a joint

study on strategies to counter disinformation that ECU and UC are progressing under a Defence grant.

Early examples of hybrid warfare have involved the coordination of insurgencies and proxies to create civil unrest. Australia embraces multiculturalism and our society reflects communities who could be considered to be **diaspora**. Although there are examples in which such diaspora have been influenced by their home nation state, we believe that the greatest threat of such relationships is more in the area of espionage than any threat of violence. The greatest physical threat comes from internal intolerant behaviour of our own citizens, rather than the real prospect of a diaspora acting against national interests. Indeed a foreign government may find it easier to influence another group than a diaspora to commit violent acts through social contagion.

Lawfare is the use of law as a weapon to achieve strategic goals by manipulating the law and changing legal paradigms. Lawfare is an emerging domain of full spectrum warfare which can either be used in its own right to achieve its own strategic objectives or as an enabler within the context of influencing the adversary in connection with well-planned information operations.[ix] It is being utilized both by Russia as part of its hybrid warfare approach[x] and by China as part of its strategic preconditioning. China's lawfare actions centre on the South China Sea, claiming that the United Nations Convention for the Law of the Sea (UNCLOS) does not provide a comprehensive approach to law enforcement issues. Actually, China considers that it may enjoy rights to protect its sovereign rights and interests as a coastal state in places like the South China Sea, East China Sea, and other maritime areas where conflict and disputes exist with non-coastal states, namely, the United States. Most of the tools China uses for preconditioning these areas are related to national and international laws.[xi] China's PLA has possessed lawfare capabilities as part of its force structure since 1996, with the US having caught up since 2001. There are two pandemic implications of lawfare for Australia: firstly, as we will expand later, opportunistic countries may exploit lawfare in combination with other hybrid activities while the world is distracted with the pandemic; and secondly, arguably Australia needs to develop lawfare capabilities to counter adverse activities.

Hybrid threats include the full array of tools that may be exercised by a nation, including **diplomatic power**. Foreign aid is a key element of diplomatic power and it would be easy in a pandemic to reduce priority to foreign aid in the face of demands from one's own population, such as in the supply of medicine and equipment. Whilst we have no visibility of the level of Australia's assistance during the pandemic (other than DFAT general advice on the Step-Up program), Australia did provide responsive disaster relief after Cyclone Harald in April. Such assistance is important to regional stability and security, especially in the face of geopolitically-motivated assistance to regional nations from China[xii].

On the topic of such assistance, although not directly pandemic related, the financial programs associated with the **CCP Belt and Road Initiative** represent a diplomatic tool being used to extend Chinese power. Australia should not interfere with other nations' decisions on joining the BRI, however the Victorian Government's BRI status undermines the Federal Government's ability to manage foreign affairs on behalf of the Commonwealth, which could have further implications for Australian policies and mitigations in future.

Another diplomatic power implication from the pandemic is that the Government should consider how best to frame communications around sensitive matters such as the need for an investigation. Although such an investigation is critical to help mitigate future impacts of a pandemic, the outcome might best have been achieved without such a truculent manner, preferably avoiding the tension and trade impacts.

This leads to the matter of **economic coercion**. The CCP's apparently retaliatory imposition of constraints on barley and beef exports impacted Australia's economy, but more importantly highlighted the significant broader vulnerability of our economy to such coercion. Economic coercion may be a highly effective tool during a pandemic, as the economic impact of a pandemic may cause governments to be less resilient to threats of further economic damage from trade conflict. We have seen how China is using trade and foreign investment as coercion against states questioning the pandemic origin or anything else that they interpret as criticism. We have seen resilience in the face of adversity when Australia and its allies publicly vowed not to bow to China's extortion.[xiii]

A key consideration by the Committee is to balance the risks and rewards of this **trade dependency.** On one hand there is an argument to pursue greater diversification to hedge against the risk of coercive behaviour. There is a counter argument that we should continue to maximise trade benefits of exports to China, accepting the risk of exports being affected if the relationship deteriorates; cognisant that in many cases such a situation may also affect China as the importer. One important factor may be the flexibility of sourcing alternative markets, which may vary across the suite of exported goods and services. If there is such variability, then we may see different sectors taking different approaches to diversify or remain as-is, rather than a one-size-fits-all strategy.

An obvious implication of a pandemic is the resultant impact on the **movement of people**. Whereas other economic activity may resume after a period of disruption, the threat of pandemics may have longer term influences on activities that rely on travel. The biggest impacts to Australian trade of a pandemic therefore are associated with education and tourism/travel, representing the nation's third and fifth biggest exports respectively. While increased tension with other nations (such as we have seen as part of China's retaliation) may impact these aspects of the Australian economy, the much greater potential is the prospect of travel constraints due to border closures.

On tourism related travel, the only mitigation would appear to be increased effectiveness of screening measures, however there is a limit to such effectiveness given the long incubation periods associated with viruses such as COVID-19. On education and business-related travel, it is conceivable that electronic systems may provide alternatives, however the value of international education is unlikely to be maintained without face-to-face delivery. Australia's universities have become dependent on this revenue: if this is threatened, the academic sector will shrink unless an alternative can be identified.

In addition to exports, the pandemic has also highlighted vulnerabilities in our imports – that is, the critical dependencies of our **supply chains** on foreign sourced materials. The most obvious and direct example of this has been in medicines and medical

equipment. If the pandemic had resulted in extended loss of supplies through interruption of sea and air lines of communication, through closure of production in foreign nations or through trade-impacting tensions, the impact on our economy and society could be significant.

An important consideration for the inquiry therefore should be whether to examine our supply chains in more detail, to identify those supplies that are associated with critical capabilities, both economically and societally. The concept of critical infrastructure should be expanded to encompass such supply chains, and the dependencies on foreign supplies should be analysed to determine the level of risk and whether it may be viable and justifiable to shift to sovereign supply or increase minimum levels of stock, even if this means we need to pay a premium.

Additionally, even in supply chains that do not support critical activities, a review of imports might uncover opportunities for Australia's industry to resume production or processing where it was previously considered uneconomic. For example, in many industries the previous barriers of labour costs may be less relevant now and in future with increasing levels of automation. Review of future strategic industries may also result in more sovereign capabilities, such as lithium batteries and rare earths.

With the centrality of the information environment to the future economy, **information technology** supply chains are particularly relevant. The Government has provided direction in relation to 5G technology, in recognition of the risk of this core technology being manipulated, with a concern more for the confidentiality, availability and integrity of systems and information than the supply of components.[xiv] In this regard, it is not viable to take a sovereign approach to all IT, or even those associated with critical functions. However, we can and must introduce arrangements to not only have trusted supply chains for critical information infrastructure, but also where appropriate to have sovereign cyber protection arrangements utilising the small but growing Australian cyber security industry.

Such a requirement is not solely driven by the prospect of a pandemic, but due to the broader geopolitical tensions that exist and will continue into the foreseeable future. As we have seen in the first half of 2020, these tensions are amplified by a pandemic event and place greater potential for grey zone conflict involving cyber and disinformation attacks on our infrastructure and social cohesion. In order to deal effectively with a pandemic threat, we need clarity and accuracy of our information systems and in communications with our citizens, hence resilience of our information systems should be a high priority for government.

With the economic impact and higher public debt resulting from the pandemic, one option to help improve the economy may be to reduce government spending, including **defence spending**. However, the geostrategic environment is less stable than any time in recent history and a reduction in military spending would be unwise. Australia needs a credible defence capability, but not necessarily the one currently planned. A new Defence strategy is needed that not only considers this new strategic reality, but considers what future capabilities are needed, including the ability to deal more effectively with grey zone threats. These capabilities should be supported where possible with sovereign supply chains, whereas our defence acquisitions typically

have little Australian industry content. Increasing AIC content is needed both from a sovereignty perspective but also to help boost the Australian economy.

A specific consideration for Defence is to consider the prospect of a non-state or state actor deliberately spreading a pandemic. While **CBRN** protection has been a minor consideration in Defence planning, it primarily has been associated with tactical scenarios. An implication of COVID-19 may be that the ADF and the nation might need to prepare for the terrible prospect of a deliberate pandemic threat within a more strategic biological warfare scenario. That prospect of a weaponization of pandemics is a difficult subject but one that demands attention.

There is the risk that other nations may use this and future pandemics as **opportunities** to further unpopular objectives and national interests whilst the rest of the world is distracted. This prospect is also often discussed in terms of a weaponization of COVID-19, albeit it is more about opportunism than actually weaponizing the virus.[xv] The strongest example of this is China, with actions continuing on the BRI program, the integration of Hong Kong, the development of facilities in the South China Sea, the current border crisis with India, the challenging of Taiwan and most recently the cyberattacks against Australian government, businesses and critical infrastructure.

These activities reflect that the Chinese Government in particular is taking advantage of the pandemic to pursue objectives that have regional and global implications, not just implications for Australia. While geopolitical strategies such as the US policy of containment would only exacerbate relationships with China, a global partnership that helps rebuild economies in a responsible and altruistic way should be a common interest for nations.

What we need now is a new comprehensive approach with our strategic partners in the region and our traditional security partners of the Five Eyes and in Europe. We should work toward the idea of a post COVID-19 'Marshall Plan 2', where like-minded nations can work together towards a comprehensive partnership for freedom and prosperity. Such a plan would help nations recover from the pandemic and its human and economic cost, but also promote alternatives to China's plan for new global order[xvi].

Conclusion

The dominance of information systems in modern society and globalisation of trade has created an environment in which our nation is increasingly vulnerable to a range of hybrid threats; many of which are being waged on a regular basis under the threshold of warfare, and often as covert or non-attributable activities. The occurrence of a pandemic has created additional chaos and motivation for these threats to become even more prominent and dangerous.

COVID-19 has laid bare vulnerabilities due to Australia's overdependency on China as a trade partner, our inaction on influence activities and erosion of our sovereignty[xvii]. The current Chinese trade sanctions, diplomatic threats and ongoing cyberattacks against Australia for having called for an independent inquiry into the origins of the

coronavirus highlight this vulnerability and the threat of coercion. As much as we should be concerned with the threat of pandemics to the safety and security of our population, we believe this threat is exacerbated by the prospect of an aggressive and opportunistic China and the structural vulnerabilities of our trade and supply chain arrangements. It is critical that we increase our resilience in the face of economic coercion and political interference by China, with whom our future relations must come from a position of unity and strength[xviii].

Dr Andrew Dowse AO is the Director of Defence Research and Research Leader Information Warfare at Edith Cowan University. Before starting in this role in early 2018, he had a 37 year career with the Royal Australian Air Force as an electronic engineer, reaching the rank of Air Vice-Marshal.

Dr Sascha Dov Bachmann is Professor in Law at the University of Canberra and a Fellow of NATO SHAPE for the Asia Pacific (Hybrid Threats and Lawfare). He was the Subject Matter Expert (Cyber and Law) for NATO Allied command Transformation's Countering Hybrid Threat Experiment (CHT) in 2011 and has published more than 40 articles on the subject of Hybrid Warfare and Greyzone..

Perth and Canberra,19 June 2020

---

[i] See https://www.minister.defence.gov.au/minister/lreynolds/speeches/aspi-international-conference-war-2025 and https://www.aspistrategist.org.au/adf-chief-west-faces-a-new-threat-from-political-warfare/

[ii] For an explanation of grey zone and hybrid warfare, see https://www.themandarin.com.au/110150-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone/

[iii] Consistent with Ashby's Law of Requisite Variety

[iv] Sascha Dov Bachmann and Hakan Gunneriusson, "Russia's Hybrid Warfare in the East – the Integral Nature of the Information Sphere, *Georgetown Journal of International Affairs* 2015, 198

[v] https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2145001/chinas-strategic-preconditioning-in-the-twenty-first-century/

[vi] http://www.fletcherforum.org/home/2020/5/13/how-china-uses-strategic-preconditioning-in-the-age-of-great-power-competition

[vii] Such as the theory of 5G enabling spread of the virus

[viii] Such as Twitter's removal of Chinese accounts, see https://www.bbc.com/news/business-53018455

[ix] https://www.tandfonline.com/doi/full/10.1080/09546553.2018.1555975

[x] http://www.jwc.nato.int/images/stories/_news_items_/2017/Lawfare_Moore.pdf

[xi] http://www.fletcherforum.org/home/2020/5/13/how-china-uses-strategic-preconditioning-in-the-age-of-great-power-competition

[xii] See https://www.lowyinstitute.org/publications/china-coronavirus-aid-pacific-islands-part-geopolitical-game

[xiii] https://www.aspi.org.au/opinion/why-australia-must-not-bow-china-seek-wider-trade-options

[xiv] https://theconversation.com/why-huawei-security-concerns-cannot-be-removed-from-us-china-relations-116770

[xv] https://vnexplorer.net/how-china-weaponizes-covid-19-in-the-east-vietnam-sea-a202029303.html

[xvi] https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order

[xvii] https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2178205/the-silent-erosion-of-sovereignty-a-sinoaustralian-example/

[xviii] https://www.defenceconnect.com.au/key-enablers/5792-insight-australia-s-relationship-with-china-andrew-hastie-mp