YOUNG AUSTRALIANS in
INTERNATIONAL AFFAIRS

IMPROVING AUSTRALIA'S GREY ZONE DEFENCES

POLICY BRIEF - JAMIE SPITERI

EXECUTIVE SUMMARY

The ‘Grey Zone’ describes efforts made by countries to coerce others without risking military retaliation. It is a complex, multi-faceted, new age theatre of war that cannot be addressed adequately by reinforcing conventional war fighting capabilities.

The 2020 Defence Strategic Update (the Update) identifies the Grey Zone as a serious threat to Australia. It frames the competition between the United States and China in the Indo-Pacific as the greatest risk to stability in the region while simultaneously reinforcing Australia’s commitment to the US-Australia alliance. The Update therefore clearly implicates China as Australia’s key adversary moving forward. [1]

An important consideration when constructing defence forces is the type of threats that must be defended against. The Grey Zone threats that Australia has faced from China in recent years have been both regular and costly, taking their most recognisable shape in the form of cyber-hacking, economic coercion, risks of debt-trap diplomacy,[2] ‘salami slicing’ of contested geopolitical regions,[3] disinformation campaigns,[4] and controlling of strategically critical infrastructure such as the Port of Darwin.

This brief recommends three policies to strengthen Australia’s defence forces against unconventional Grey Zone threats:

1. Expand the Australian Civil-Military Centre (ACMC) to train key individuals in military strategy and public administration;

2. Create a civilian cybersecurity volunteer institution; and

3. Desist with Department of Foreign Affairs and Trade (DFAT) funding cuts.

BACKGROUND

In 1999, two officers of China’s People’s Liberation Army (PLA) presented a doctrine known as ‘Unrestricted Warfare’ (URW), which was intended to broaden the scope of warfare beyond traditional military engagement. URW advocated the weaponisation of non-military aspects of society such as technology, information, commerce, education, communications and the international system itself,[5] intended to create asymmetries in China’s favour. Additionally, URW sought to attack China’s adversaries at a level below the traditional military escalation point, thereby reducing the chances of retaliation. [6]

Over the last two decades, China’s increased economic clout has directly translated into more aggressive foreign policy which has incorporated URW. In the Australian context, this was recently outlined by China’s dossier released last year, which listed ‘14 grievances’ undertaken by Canberra. [7] Actions such as banning Huawei from sensitive technological infrastructure and supporting international law over the South China Sea were listed, with each additional point on the dossier encompassing a different facet of URW. The list saliently outlined ways that China attempted to create or exploit asymmetries in its favour beneath the level of military escalation.

The Australian government addressed unconventional URW threats in the 2020 Strategic Update; however, the update substituted the phrase ‘Unrestricted Warfare’ with their preferred term; the ‘Grey Zone'.

THE PROBLEM

Australia’s strategic adversaries are using offensive methods which blur the line between military and civilian space, yet Australia is ill-equipped to defend this space. To increase overall Grey Zone defence, the military needs to work more closely with civilian elements of Australia’s national security. [8]

However, the Australian Defence Force (ADF) has been growing parallel to resources and funding cuts in the civil service, particularly DFAT. Consistent bipartisan funding cuts have limited DFAT’s ability to operate overseas in an effective diplomatic capacity. This undermines Australia’s ability to shape its external environment, one of the key strategic components of the 2020 Update. [9] These trends have increased the militarisation of Australian foreign policy and diplomacy. This is highly problematic, as framing countries as a threat increases the likelihood that they become one. [10]

Grey Zone attacks also come with a large financial cost. In 2019 alone, cyber-attacks had an estimated cost of AUD$29 billion to the Australian economy. [11] This will increase as cyber weapons become cheaper and more accessible. Further, an over-reliance on Chinese two-way trade enables the Chinese Government to weaponize bilateral commerce. It has done this on several occasions with commodities such as coal, lobster, and wine. [12]

While the Update pioneers the concept of the Grey Zone, it falls short in recommending tangible steps to combat the problems listed above.

POLICY RECOMMENDATIONS

1 EXPAND THE AUSTRALIAN CIVIL-MILITARY CENTRE (ACMC) TO TRAIN KEY INDIVIDUALS IN MILITARY STRATEGY AND PUBLIC ADMINISTRATION

Effective Grey Zone activities occur at the civilian level yet have militaristic aims. As such, it is necessary for key individuals (politicians, ADF officers, and public servants) to have a pronounced understanding of this nexus. Training ADF officers to recognize the civilian aspects of warfare while simultaneously training public servants to recognize the potential military implications of seemingly benign activities such as trade will create an environment in which key decision-makers and advisors are well placed to react.

The ACMC is the natural home to lead on such an initiative. It has existing institutional cross-over between domestic, international, and ADF operations and offers ready-made linkages between civil servants and the military. However, the ACMC needs to be expanded beyond its current obscurity and thrust into a key instructional role, working to fill the current vacuum that exists in Australia’s Grey Zone capabilities.

Importantly, training public officials in the significance of every role in the ACMC will combat the tribalism that can form not only in each of the three arms of the ADF, but also in the public sector.

Investing in Australia’s heavy land capability or expanding the cyber-response capabilities of the Australian Signals Directorate (ASD) are valuable initiatives for increasing national security, but not if they come at the expense of DFAT, and not if they have been paid for with international trade that creates further vulnerabilities. Recognizing the holistic framework of national security is crucial and requires a holistic array of stakeholders.

2 CREATE A CIVILIAN CYBERSECURITY VOLUNTEER INSTITUTION

Cyber-attacks on Australia are persistent, regular, and extremely costly. While this has been recognised and the government has outlined an AUD$15 billion increase in cyber capabilities over the next decade,[13] creating a civilian cyber volunteer institution is a low-cost way to vastly decrease Australian defence vulnerabilities in this area. Additionally, cybersecurity volunteers would help to improve state, territory, and local cyber resilience, as no capacity currently exists outside of federal agencies. [14]

Training a base of cybersecurity volunteers is a low-cost way to inflate the base of Australians with useful skills to help defend Australia’s cyberspace, which is a key facet of the Grey Zone and ultimately helps to improve Australia’s cyber response capabilities.

3 DESIST WITH DFAT FUNDING CUTS

Consistent bipartisan reductions in DFAT funding have weakened Australia's diplomatic capacity at a time when it is highly needed. Australia will need to invest in its diplomatic capacity in order to build stronger regional security and economic relationships, especially with fast-growing Asian and Pacific Island State economies.

Building relationships with many of these countries has proven to be tumultuous in times past. Indonesia, for example regularly exhibits caution in forging stronger ties with international partners due to their colonial history. [15] Improving bilateral relations with key international partners such as Indonesia presents a formidable task when attempted with reduced DFAT capacity.

The benefit of stronger trade relationships with diverse partners is a decreased reliance on exports to China. Australia is seemingly well placed geographically to take advantage of growing markets, especially those in India and Indonesia, both of which are projected to enter the list of the top five world GDP countries by 2050. [19] This is not a recommendation to reduce overall trade with China. Rather, increasing trade with other countries would decrease the percentage represented by Chinese trade alone thereby reducing Australia's susceptibility to economic coercion.

CONCLUSION

Initiating these policy recommendations will increase Australia’s Grey Zone operational ability. As the Grey Zone is the specific area between the military and the civil, which is also the area that China has effectively weaponised under URW, these recommendations are timely and important. It behoves those involved with the defence of Australia to focus on areas of vulnerability and to address them appropriately. Increasingly, this is no longer the purview of the ADF alone.

Finally, while this paper has focussed specifically on China as the most salient of contemporary Australian adversaries in the Grey Zone, executing the recommendations outlined above will help Australia in its defence against any adversary.

Jamie Spiteri

Jamie holds a Bachelor of International Relations from La Trobe University, and is currently studying a Master of Laws at ANU. He currently works as a Security Advisor for Hanwha Defense Australia, and is primarily interested in exploring modern and irregular forms of warfare

REFERENCES

[1] Department of Defence. 2020 Defence Strategic Update. Canberra, 2020, available from: https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf

[2] Rajah, Roland, Pryke, Jonathan & Dayant, Alexandre. China, the Pacific, and the “debt trap” question. Lowy Institute [Internet]. 23 October 2019. Available from: https://www.lowyinstitute.org/the-interpreter/china-pacific-and-debt-trap-question

[3] Raaymakers, Steve. China expands its Island-building strategy into the Pacific. ASPI, The Strategist [Internet]. 2020 [cited 2020 September 11]. Available from: https://www.aspistrategist.org.au/china-expands-its-island-building-strategy-into-the-pacific/

[4] Morrison, Sarah, Barnet, Belinda & Martin, James. China’s disinformation threat is real. We need better defences against state-based cyber campaigns. The Conversation [Internet] 2020 (cited 2020 June 24). Available from: https://theconversation.com/chinas-disinformation-threat-is-real-we-need-better-defences-against-state-based-cyber-campaigns-141044

[5] Liang, Qiao, Xiangsui, Wang. PLA Literature and Arts Publishing House, Unrestricted Warfare, trans. Foreign Broadcast Information Service (FBIS), (Beijing, 1999). Available from: https://oodaloop.com/documents/unrestricted.pdf

[6] Kilcullen, David. Dragons and the Snakes: How the Rest Learned to Fight the West. Brunswick, VIC: Scribe Publications; 2020

[7] Dobell, Graeme, ‘Fourteen points on Australia’s icy times with China’ ASPI, The Strategist [Internet]. 2021 (cited 2021 April 6). Available from: https://www.aspistrategist.org.au/fourteen-points-on-australias-icy-times-with-china/

[8] Department of Defence. 2020 Defence Strategic Update. Canberra, 2020. 5 p. Available from: https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf

[9] Ibid 24-25 pp.

[10] O’Keefe, Michael. The Militarisation of China in the Pacific: Stepping up to a New Cold War? Security Challenges [Internet]. 2020; 16(1): 94-112. Available from: https://www.jstor.org/stable/26908770?seq=1#metadata_info_tab_contents

REFERENCES

[11] Harvey, Jillian. Cybercrime costs Australian Businesses $29 Billion a year [Internet]. Agilient. 2020 (cited 2020 October 3). Available from: https://www.agilient.com.au/2019/10/23/cybercrime-costs-australian-businesses-29-billion-each-year/#:~:text=The%20Morrison%20Government%20estimates%20cybersecurity,survey%20results%20released%20mid%2D2019

[12] Grigg, Angus, Smith, Michael, Thompson, Brad & Tillett, Andrew, 'China targets $6b of Australian exports in fresh campaign [Internet]. Australian Financial Review. 2020 (cited 2020 November). Available from: https://www.afr.com/world/asia/china-targets-6-bln-of-australian-exports-in-fresh-coercian-campaign-20201103-p56ayx

[13] Department of Defence. 2020 Defence Strategic Update. Canberra, 2020. 35-36 pp. Available from: https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf

[14] Mansted, Katherine & Robinson, Finn. Australia needs volunteers to be ready for a cyber conflagration [Internet]. ASPI, The Strategist. 2020 (cited 2020 May 22). Available from: https://www.aspistrategist.org.au/australia-needs-volunteers-to-be-ready-for-a-cyber-conflagration/

[15] Bland, Ben. Man of Contradictions: Joko Widodo and the struggles to remake Indonesia. Melbourne: Penguin; 2020

[16] PricewaterhouseCoopers. The World in 2050 Will the shift in global economic power continue? [Internet]. 2015 (cited 2015 February). Available from: https://www.pwc.com/gx/en/issues/the-economy/assets/world-in-2050-february-2015.pdf

YOUNG AUSTRALIANS in
INTERNATIONAL AFFAIRS

POLICY@YOUNGAUSINT.ORG.AU