AUSTRALIAN CRISIS SIMULATION SUMMIT WORKING PAPERS

VOLUME 1
NOVEMBER 2021

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

DIRECTOR'S FOREWORD

Gemma Dabkowski

Dear Stakeholders,

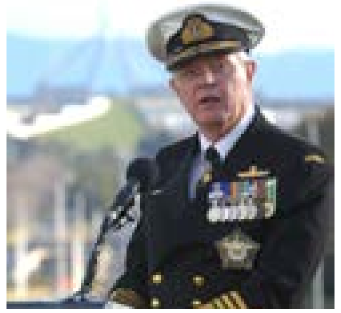
I am pleased to support the publication of the inaugural Australian Crisis Simulation Summit (ACSS) Journal. Published in collaboration with the Crawford School of Public Policy at the Australian National University, it brings together writing from academics, industry professionals and most importantly our student delegates who participated in the ACSS simulation exercises in 2020 and 2021. Covering a broad range of topics from climate security to space, this is an opportunity for engaged members of the broader national security community to share their opinions and research. The national security landscape in Australia is shifting. We are facing new threats and challenges including cyber-enabled foreign interference, flooding and other extreme weather events and the formation of new security agreements in the Indo-Pacific region. This will require us as Australians to challenge old assumptions and generate new solutions to safeguard our national interest. I invite you to consider and reflect on what is being proposed in this Journal, in particular the articles from ACSS student delegates. These young Australians bring a unique perspective to the national security conversation, and are eager to continue these discussions into the future.

GEMMA DABKOWSKI

2021 Director of the ACSS

PATRON'S INTRODUCTION

Admiral (Ret.) Chris Barrie AC



"It is not the critic who counts, not the one who points out how the strong man stumbled or how the doer of deeds might have done them better. The credit belongs to the man who is actually in the arena, whose face is marred with sweat and dust and blood; who strives valiantly; who errs and comes short again and again; who knows the great enthusiasms, the great devotions, and spends himself in a worthy cause; who, if he wins, knows the triumph of high achievement; and who, if he fails, at least fails while daring greatly, so that his place shall never be with those cold and timid souls who know neither victory nor defeat." Theodore Roosevelt, extract from The Man in the Arena, 23 April 1923.

This quote from former president of the United States of America Theodore Roosevelt points to the fact that until we find ourselves in positions of high authority, we cannot know what it is really like to be appointed to positions of huge responsibility and accountability in framing and executing responses to complex national security challenges. Yet, in through a series of scenario games in the Australian Crisis Simulation Summit, that is exactly what we are trying to do. We use complex scenarios, developed by clever people in crisis writing teams, to set the scene in a gaming environment and give Summit delegates a feel for what it might be like to be advisers and decision-makers responding to national security crises.

There are no straight forward and easy solutions to any of these challenges.

It was my privilege as patron to support the first Australian Crisis Simulation Summit in 2020. As a start-up event it delivered beyond my expectations. Now the bar has been set high. I am looking forward confidently as patron to the delivery of a brand-new Australian Crisis Simulation Summit in 2021 — one that includes a different set of credible scenarios that will surpass the experience of last year in presenting challenges for the delegates.

When I look into the next decade, I can see a world that is full of new and more complicated challenges that will need to be solved. They are all wicked problems — whether these be state failure, climate change consequences, the race to defeat new viral diseases, breakdowns in law and order within states, tension created by food and water scarcity, space security, or dealing with the rise of China.
The new generation of leaders in Australia, and around the globe, will have to step up into key leadership roles equipped with a full suite of leadership skills. They will have to make the best calls on what needs to be done to solve an array of pressing problems.

My interest in war games began in the mid-1980s. Since that time, I have been involved in many games — as a player, in small games involving less than 10 people, and large games involving several hundred people, as well as seeing the development of sophisticated technologies to support gameplay. I have also been a game creator and director.

I introduced the use of scenario games in the Department of Defence when I became Chief of the Defence Force (CDF) in 1998 and within the Australian government shortly afterwards. Our games involved the political leadership and the various departments and agencies at the federal level, as well as with state and territory counterparts. This kind of gaming is still in use today to enhance preparedness for unexpected scenarios.

Participants in the Australian Crisis Simulation Summit, of course, are not going our current policy and decision-makers. But given that we learn best from doing, the delegates in the simulation exercises will feel some of the pressures that the current national security leadership team experience. They will have the opportunity to share their thoughts and perceptions with mentors and other senior advisers from the government, academia and business who can advise them from their practical experience, enhancing the Summit experience.

I do hope that everyone participating in this year's crisis simulation will appreciate the importance of each other person's contribution in trying to find appropriate answers in these highly challenging circumstances. All good scenario games depend on each participant trying their best to play a role faithfully whilst learning from the insights of others. It is also part of a good scenario dynamic that solutions are not pre-cooked.

I would expect that over time, delegates will reflect and continue to learn from their experience in the Summit. They may come to think, as I have done in my own life, that the scenario was not quite right, or that they went around trying to solve the problem in the wrong way. Sometimes, it can be many years later when the light dawns that the solution to a particular problem was in fact to approach it from a completely different perspective. In my view, this illustrates the importance of learning by doing.

For all these reasons, I extend my full support 2021 Australian Crisis Simulation Summit, and look forward to further engaging with those involved to discover what key insights people have gained.

Admiral (Ret.) Christopher Alexander Barrie, AC is the former Chief of the Defence Force of Australia and Honorary Professor at the Strategic and Defence Studies Centre at the Australian National University.

IS AN AUSTRALIAN NATIONAL SECURITY STRATEGY POSSIBLE?

William A. Stoltz,
Australian National University

In recent times there has been renewed discussion about the need for a new national security strategy for Australia — that is to say, the need for a single formal document drafted by the Commonwealth public service, sponsored by a minister or the prime minister, endorsed by Cabinet and disseminated publicly and within government for implementation. Certainly, the wicked problems and plausible crises explored through the Australian Crisis Simulation Summit show that more strategic planning, coordination, and responses are required to support whole-of-nation security, but is achieving an effective Australian national security strategy in this way actually possible? This piece outlines the range of structural, cultural, and cognitive obstacles to creating and implementing such a formal strategy. It concludes that a useful national security strategy is not obtainable for Australia under present circumstances. Instead, the way for Australia to achieve higher levels of strategic coherence in how it undertakes national security activities lies in maintaining a diverse system of strategic forums that convene key stakeholders, provide avenues for greater understanding of multi-faceted national security problems, and deepen the essential networks across governments, the private sector and civil society that are required to coordinate Australian society to be more resilient and secure.

Why a formal strategy?

Australia's approach to setting national security strategy has generally involved the drafting of formal policy documents typically concerning a discreet aspect of national security policy. The foremost of these documents have been 'white papers' — lengthy statements of the Australian Government's strategic objectives for a given security portfolio, which are produced by the public service before being endorsed and released by the Cabinet. These white papers typically comprise a version for public release as well as a classified version for government consumption. The first such white paper for an area of Australian national security policy was the 1976 Defence White Paper, which outlined Australia's policies for military security out to approximately 1981. The need for such a document was generated, in part, by the United Kingdom's 1966 British Defence Review, which articulates a comprehensive strategic vision for the British military that saw a significantly down-scaled presence 'East of Suez'. This document not only outlined a British strategy that meant that Australia needed a plan for more military self-reliance, but it also provided an example of the kind of long-term strategic planning documents that the Australian public service could replicate.

Since the 1970s, Australian governments have followed this white paper model to articulate long-term strategic objectives and priorities for other areas of national security policy as well, with the 1997 Foreign Policy White Paper outlining objectives for international security. These portfolio-centric white papers have occasionally been complimented by similar strategic documents that articulate aims across portfolios, such the Rudd government's National Security Statements and the 2012 Asian Century White Paper and the 2013 National Security Strategy released under the Gillard government.

The use and usefulness of these kinds of formal strategy documents is debateable. Within government such documents and their classified iterations ostensibly provide a clear reference for the objectives of the government of the day to guide the more detailed work of different portions of the public service. However, given strategic documents like white papers articulate objectives and policies in such broad overarching terms, seasoned public servants can typically 'link' whatever work they like to these strategies through creative re-interpretation.

The tabling of these documents in Parliament allows for the government to publicly explain its strategic objectives, and for the opposition to hold them accountable. Public release can also be valuable for informing the work of industry, academia, and the media. However, formal strategic documents by no means have a monopoly on this function, with well-placed speeches, articles, and media engagements by ministers potentially having the same effect.

Wither the white paper

There are several reasons the Australian government's traditional approach to strategy-making is not well suited to developing and

implementing an overarching national security strategy. For one, some of Australia's key political institutions and governmental structures do not lend themselves to cohesive, centralised strategic direction-setting by the Commonwealth on all security issues. Also, the nature of Australian politics obstructs robust long-term strategic planning and inhibits the ability of otherwise powerful executives, like ministers or prime ministers, from practicing unilateral leadership of whole-of-nation security. Further, the dynamism and complexity of the domestic and international threats to Australia's security in the twenty-first century demand responses that cannot reliably by planned through a singular national strategy.

Australia's current and foreseeable strategic environment will primarily be dominated by threats enabled by technology, that transcend domestic and international realms, and feature the co-mingling of malicious state and non-state actors. The expanding frontier of malicious cyber attacks by states and criminals; burgeoning foreign interference into all aspects of Australian society; and the growth in an ever-widening range of violent ideologies, are but a few examples of the most pressing and intractable threats. Pre-empting and responding to these types of technology-enabled threats that transcend traditional borders not only demands strong international collaboration, but for Australia it also requires the highest degrees of collaboration and interoperability between all levels of government, the private sector, and civil society. Accordingly, in this context a formal Commonwealth national security strategy arguably cannot be expected to succeed when the Commonwealth itself does not have all the knowledge, capabilities, or legal authorities to impose and direct such a strategy. For example, Australia's pandemic response has highlighted that regarding biosecurity threats, Australia's state governments still retain extraordinary legal power and responsibility for essential operational aspects, making the imposition of a centralised Commonwealth strategy unfeasible, hence the creation of the National Cabinet.

Other structures and institutional arrangements make the accomplishment of an Australian national security strategy by the Commonwealth doubtful. For one, the most powerful figure in national security strategy-making, the Prime Minister, is not a codified office; with the Constitution being silent on the powers of the PM. Accordingly, the ability of the PM to exercise executive leadership over the nation's security — the real extent of their unilateral power — is highly susceptible to the peculiar idiosyncrasies of how they have achieved and maintained their leadership position within the Cabinet and the wider party of government. The extent to which Prime Ministers can exert their executive authority will, to varying degrees, always be subject to the degree of real power they have relative to the influence of their Cabinet colleagues; the desires of their parliamentary party membership; and the wider national party apparatus. It is for this reason that achieving consensus within the Commonwealth's Cabinet is critical to the accomplishment of a strategy for any policy area, as without a sense of ownership by the whole Cabinet a strategy may just as soon be discarded with an out-going minister or Prime Minister, as was the case with the 2013 National Security Strategy that was introduced by Julia Gillard but largely shelved upon the re-ascension of Kevin Rudd later that same year.

This leads us to a key characteristic of Australian strategy: a strategy must ultimately reside in the mind of the minister. The bureaucratic processes that have surrounded Australian strategy-making for the past forty years or so — the drafting of formal white papers by departments and the official endorsement of these documents by government — have obscured the reality that national strategies are inherently political edifices, leading some to believe that publishing a document or white paper equates to the true creation of a national strategy. The public service can advise on strategy, but whether it is truly implemented depends entirely on the ability and willingness of a patron minister to understand it, own it, argue for it within Cabinet, and advocate for it to the wider party, Parliament, and the public. In the context of the political factors mentioned earlier, and structures like three-year Federal parliamentary terms, the realisation of a national strategy on anything as long-term and complex as national security appears highly unlikely. So how then can we achieve a more strategic approach to national security without such a formalised edifice?

Towards Strategic Behaviour

Rather than measuring the efficacy of Australia's approach to national security according to whether it does or does not accord with a centralised, formalised 'strategy' from the Commonwealth, we should instead focus on ensuring that the disparate strands of work that support Australia's security are broadly aligned with the same appreciation of what Australia's national interests are. This way, while Australia's overall national security might not be centrally directed, it would at least be supported by 'strategic behaviour' from government, industry, and civil society stakeholders, respectively. Curiously enough, Australia's old approach to considering strategic security issues prior to the era of white papers may offer a guide for how Australia can at least achieve a higher degree of strategic behaviour in the modern era.

Rather than believing that a formal national security strategy will provide the whole-of-nation approach to security Australia needs, we should instead focus on establishing formal and informal forums and networks that regularly convene stakeholders from across the jurisdictions of Australian government, the private sector, and civil society institutions to build a consensus understanding of Australia's national interests and the threats to them. A focus on building forums and networks that inculcate a strategic consciousness among members, and strategic behaviour within the organisations they lead, may sound like a nebulous, untested way in which to achieve our security, but in fact it is much closer to how Australia's international and security policies were coordinated for most of the twentieth century.

From Federation through the late 1960s, when Australia's security and international role was interlinked with the British imperial system, Australia's strategic approach to security was devised and shaped within a constellation of imperial, multilateral decision-making forums representing the nations of the British world. Bodies like the Imperial Conferences, the Committee of Imperial Defence, the Imperial War Cabinets, and the ANZAM joint staff meetings, convened key leaders and functional decision-makers with a view to establishing a common strategic understanding between all governments and, importantly, reaching a shared consensus on what the objectives and security interests of the imperial system were. None of these bodies had the ability to formally bind a national leader to a certain course of action, but rather by inculcating a sense of shared security objectives they allowed strategic behaviour among the imperial states to occur.

This style of 'strategy by consensus' would appear well-suited to Australia's largely uncodified, federated structures of national power as well as the cross-jurisdictional nature of the modern security threats with which we must contend. This model of strategic inculcation could be tested by forming councils or networks of appropriate leaders from stakeholder bodies around specific national security problems, such as foreign interference, cyber security, or biosecurity. Achieving 'strategic behaviour' via this method, however, would likely require a cultural step-change from the Commonwealth to accept the role of convenor and moderator, as opposed to executive director. Overcoming the threats to Australia's future will therefore demand humility as a well as innovation.

William Stoltz is the Senior Adviser for Public Policy for the National Security College at The Australian National University.

LESSONS IN CRISIS MANAGEMENT: THE EP-3 CRISIS

Anastasia Kalloniati,
Australian National University

Negative perceptions of international security and relations between global powers are steadily rising with mounting tensions between the United States and China. In this fearful climate, we need to look deeper at crises that had the potential to be devastating, but were not, to better tackle those that may arise in the future. The EP-3 crisis is a fascinating case that fits this description.

The events of the EP-3 crisis are still contested. On 1 April, 2001, a 24-member American EP-3 reconnaissance plane collided with a Chinese F-8 fighter jet over the South China Sea (SCS). As a result, the seriously damaged EP-3 made an emergency landing at Lingshui Military Airport on Hainan Island. China argued that the EP-3 'suddenly veered' into the F-8, causing the latter to lose control, killing the pilot, Wang Wei. Further, the EP-3's landing was unlawful as the aircraft landed in Chinese sovereign territory without permission. The United States objected, saying the EP-3 pilot would never endanger their entire crew by flying close to the F-8, whereas 'reckless' flying was characteristic of Wei. EP-3s are also large and slow, and cannot outmanoeuvre an F-8. Further, international law allows aircraft in distress to land in the territory of other states. Despite this dispute about the events, the crisis hardly seems cataclysmic. To understand what made it more dangerous we need to consider the context of the incident.

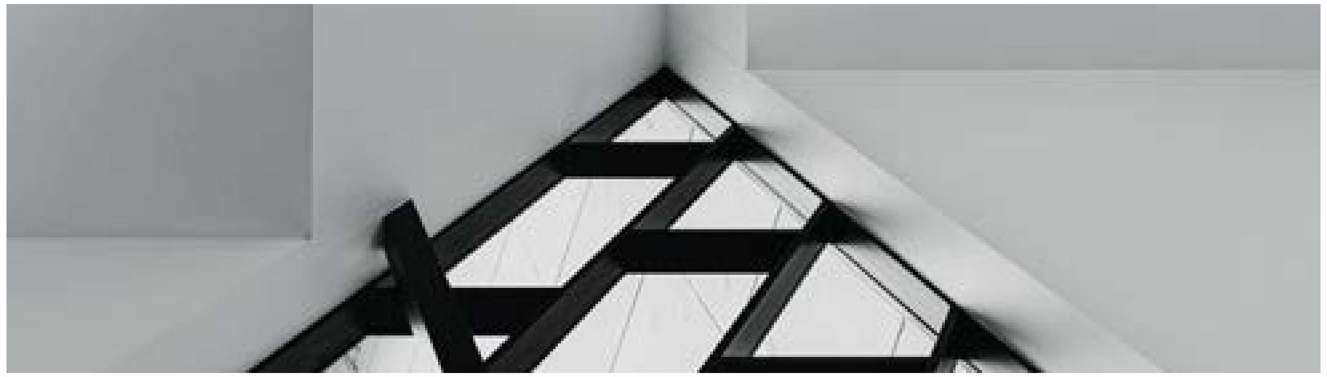
The United States and China share a tumultuous history. American support for the nationalist Kuomintang during the Chinese Civil War ensured a frosty start to the states' relations, which remained tense for decades due to Cold War politics. Confrontation in this period included two proxy wars, the first in Korea (1950-1953) and then Vietnam (1955-1975). Chinese free-market reforms and economic interdependence between the two states have reduced tensions since, but issues still erupt within the relationship periodically, and recently more so. This has included incidents such as the 1995/96 Taiwan Strait crisis and the 1999 US-NATO bombing of the Chinese Embassy in Belgrade.

One particularly prominent challenge in US-China relations lies in SCS territorial disputes. China's bold claim over the territory, which has a complicated historical justification, competes with those of numerous other states. China's asserts its control in a generous U-shaped line encompassing almost all the waters between China in the North and Malaysia in the South, and between Vietnam in the West and the Philippines in the East. This claim, also known as the Nine-Dash Line, was first published as an eleven-dash line in 1947 by a Chinese cartographer and was then circulated in its current form in 1953 by Premier Zhou Enlai. However, China has consistently asserted that the claim dates back further than the mid-twentieth century. How far back is unclear though, with some stating the second century BCE and others stating the 16th. This ambiguity has made resolving SCS border disputes difficult.

Despite their purported neutrality in the issue, the United States has routinely demonstrated a military presence in the SCS, particularly through surveillance flights. These flights were a regular occurrence in the months preceding the EP-3 crisis and were increasingly met with Chinese interceptions. The United States also implicitly supported the Philippines' claims in the SCS, the most prominent objector to China's nine-dash line, in 1998. The Defence Secretary at the time, William Cohen, upheld that the United States and the Philippines' mutual defence treaty would apply to any geographical area and that the United States was committed to defending the Philippines against any attack – including from China in the SCS. With China's fierce legal objections to American movements in the area, a crisis seemed almost inevitable.

A plane collision between two states already challenging each other's presence in the SCS could have been the proverbial straw that broke the camel's back. So why have so few people heard of the EP-3 crisis? The simple answer is that both states demonstrated efficient crisis management, meaning the event never received the broad media coverage that other global events gain.

Initially, the leaders of the United States and China faced internal pressures to pursue hard-line policies during the EP-3 crisis. There was a substantial sentiment among Americans that the policy of previous administrations towards China had been weak, and given that the EP-3 issue was President George W Bush's first major international crisis, he could not be seen making the same mistake. Indeed, a strong China policy was one of Bush's election points. Alternatively Chinese ultranationalism within the military and broader public ensured that any



anti-American policy would be in the Chinese government's political interests. Hard-line policies like these in most cases intensify, rather than de-escalate, tensions by limiting the ability of issues to be resolved through compromise.

Despite the pressure to pursue assertive policies, both states understood that continued cooperation was worth more than escalating tensions. This mutual understanding was a cornerstone of the EP-3 incident's crisis management. In particular, the American ambassador to Beijing sent the Chinese government a 'Letter of Two Sorries', expressing how 'very sorry' the US was that the crash occurred and Wei lost his life. The letter did not accept blame for the crash but was still a significant concession for the United States as apologies are generally only issued for that exact purpose.

Beijing initially rejected the letter, claiming it did not apologise sufficiently, but ultimately understood its significance and returned the EP-3 and its crew, who had been detained by China on Hainan Island. The letter also bridged cultural boundaries, with the United States recognising the symbolic importance of an apology for China, a country steeped in values of hierarchy, collectivism and deference. The letter was thus a compromise for both parties and served as an efficient method of crisis management. In this way, we can learn from the EP-3 crisis that understanding cultural and international political norms is crucial to easing tensions.

In the months following the crisis, tensions between the United States and China were also eased as another major event drew the states' attentions elsewhere — the attack on the Twin Towers (9/11). The war on terrorism following the attack provided the United States and China with a common cause for mutual aid, allowing the EP-3 crisis to recede into the background of international relations. While an event like 9/11 cannot be replicated or planned for when considering the management of future crises, it nevertheless demonstrates that states are able to waive their grievances when there are other important issues to be dealt with.

Despite effective crisis management, the EP-3 crisis did not occur without consequence. While the crisis lacked the media coverage of other internationally significant events, the attention it did receive still fuelled polarisation. Research has shown that media coverage of international crises is particularly biased when one's own country is involved. In states like China, where the distinction between government and media is unclear, this occurs more frequently.

The immediate treatment of the EP-3 crisis in both American and Chinese media followed this pattern. Media tended to follow the perspective of the government, creating a stark difference in how the crisis was being framed to the public in the two states. American sources emphasised Wei's recklessness and that the crisis occurred in international waters while Chinese sources focused on Wei's family life and martyrdom alongside the illegality of American actions. Media plays an essential role in forming public opinion which can, in turn, create domestic pressures that affect government decision-making. Therefore, the lesson we must take from the EP-3 crisis is to promote media diversity to ensure that crises are not escalated by public division.

In an increasingly tense global political climate, leaders must remember the EP-3 crisis. When states focus on cooperation and compromise, it is possible to come back from the brink. Even states with a tumultuous history like China and the United States can resolve conflicts and crises. Remembering this will be crucial in the future as the two states and their allies come into more disagreement.

Anastasia Kalloniati is a third-year undergraduate student at The Australian National University studying a Bachelor of International Security Studies and a Bachelor of Politics, Philosophy and Economics (PPE).

THE PLACE FOR 'WARGAMING' AT AUSTRALIAN UNIVERSITIES

John Blaxland,
Australian National University

Wargaming is in vogue, and not just with the military. In mid-2020, the Prime Minister appointed a senior military officer, Lieutenant General John Frewen, to head the national emergency response — a task involving planning and 'wargaming' of scenarios to help ensure the vaccine rollout proceeds as quickly and effectively as possible from here on in.

Wargaming itself is a concept long practised by the military and written about by a range of writers including The Art of Wargaming, Simulating War, and The Craft of Wargaming, among others. It has been practised in field exercises and tactical exercises without troops for generations.

As Frewen's actions demonstrate, it is also something that has been adopted for broader application beyond the military. Usually rebadged as a crisis simulation exercise, these activities have been employed by a wide range of government agencies and corporations eager to test their systems and capabilities to prepare against the risk arising from extreme environmental or human generated circumstances. Those extreme circumstances may be related to governance challenges, environmental catastrophe or great power contestational issues. They are compounded by what is described as the Fourth Industrial Revolution, and the potential for crises associated with the digital era and our reliance on technology and the World Wide Web, otherwise known as the internet.

We now live in a society that has gone from being web enabled to web dependent and, in turn, web vulnerable. Robotics, artificial intelligence, autonomous systems, satellites, drones and misinformation generated out of fear or from domestic and foreign political opportunists, are adding a degree of complexity to governance.

Reflecting this trend and capitalising on the associated opportunities, we have seen a proliferation of cyberattacks and ransomware become normalised as malevolent state and non-state actors seek to exploit vulnerabilities that have emerged in our open society.
Compounding the spectrum of challenges related to abuse of the web and advanced technology is a range of environmental concerns. The fires of late 2019 and early 2020 were followed by hailstorms, floods, pestilence and pandemic. Since then, Australian society has become more conscious of the risk arising from potential environmental catastrophe. Neighbouring societies also face significant strains in maintaining effective governance in the face of such pressures afflicting their less developed societies with less resilient infrastructure. Like a vortex, such crises can lead to demands for Australian intervention and support, often at very short notice.

The situation is exacerbated by the prospect of great power contestation more directly affecting Australia's and the region's security and prosperity than ever before. Sanctions against Australian beef, barley, wine, coal and more is coupled with growing concerns over the prospect of war over one or more of what my SDSC colleague, Professor Brendan Taylor, has called The Four Flashpoints. These include the Korean Peninsula, the East China Sea, the South China Sea and the Taiwan Strait.3 But as recent events have shown, there are plenty more in Afghanistan, Iran, Jammu and Kashmir, as well as the Line of Actual Control in the Himalayan mountains and an increasingly contested South Pacific.

The overlapping of issues related to technology, great power contestation, looming environmental catastrophe and a spectrum of governance challenges is what motivated me to write A Geostrategic SWOT Analysis for Australia.4 It also points to the utility of university students becoming familiar with crisis simulation activities or exercises. That is what some of us have done with our teaching programs. Sinclair Dineen, James Batley and Admiral (Ret.) Chris Barrie, employ a crisis simulation activity woven into their undergraduate program on Security in the Pacific. Similarly, my third year undergraduate course, 'Honeypots and Overcoats: Australian Intelligence In The World' culminates with a crisis simulation activity that takes the lessons learned from the semester's teaching and applies them for all the student participating to engage with in a realistic setting. Students are required to find creative ways to address these problems. In my experience, they have overwhelmingly valued the applied teaching methodology which seeks to enable students to look beyond the theory of many of their classes to see how some of it may work in the real world beyond the ivory tower of academia. This experience helps consolidate their learning and stretch their analytical skills.

The Australian Crisis Simulation Summit is an exciting and innovative development that seeks to take this enthusiasm for learning through crisis simulation to another level. By developing scenarios that reflect real world problems and involving real world practitioners and academics as mentors, the ACSS program has created an exciting and vibrant new platform for student led teaching and learning.

The future present enormous and complex challenges, with overlapping dimensions beyond the remit of one academic discipline, one jurisdiction or one government department. It is this interaction between legal, social, scientific and political disciplines that sees students from a wide range of universities bring their knowledge and insights together to deliver something that is more than just the sum of its parts. I am honoured and delighted to be a mentor of the ACSS and excited at the prospect of the young men and women of Australia's universities applying their knowledge innovatively to think through some of the challenges we face today, for a better future tomorrow.

John Blaxland is Professor of International Security and Intelligence Studies at the Strategic and Defence Studies Centre, The Australian National University.

THE SECURITY RISKS OF AUSTRALIA'S LANGUAGE DISADVANTAGE

Jessie Storey,
University of Queensland

On 10 September 2001 the United States' National Security Agency (NSA) intercepted intelligence of two Arabic messages sent between individuals with 'terrorist connections' . On 11 September 2001, two planes hijacked by terrorist group Al Qaeda flew into the World Trade Center in New York City, killing nearly 3000 people. On 12 September 2001, the messages were translated, one day too late. A sweeping review conducted after the attack found that the United States intelligence agencies were simply not prepared to handle the sheer volume of foreign-language intelligence they collected, resulting in significant backlogs. In fact, for the most critical languages in counter-terrorism, the National Intelligence Agencies had a readiness level of only 30 per cent.

These days terrorism is far from Australia's greatest perceived threat, but our national security faces its own linguistic battles with our increasingly aggressive neighbour, China. As the global order continues to shift, Australia must take a hard look at our language capabilities and ask ourselves if ours are any better than those of the United States nearly twenty years ago. Australia faces significant challenges in our capacity to access fluent Mandarin speakers eligible to translate intelligence from China.

According to the 2016 census, over 596,000 people in Australia speak Mandarin. So why is Australia's ability to translate Mandarin intelligence still an issue?

To be eligible to translate intelligence within Australia's national security agencies, you need the highest-level 'Positive Vetting' (or 'Top Secret') clearance, which is notoriously difficult to obtain. Applicants require a background checkable from age 16 and face a process so intrusive that prospective applicants are warned about it before they even apply. As expected, there are significant restrictions placed on persons who have, or may be perceived to have, any connection to a foreign power, including even having family, friends, or associates that are citizens or residents of a foreign country.
These restrictions make it extremely difficult for any Australians with a Chinese background to obtain Positive Vetting clearance. As said by ANU scholar Yun Jiang '[obtaining] top security vetting [is] very hard if you're born in China or have extensive family connections in China.' Since about 510,000 people in Australia were born in China (not including those born in Australia with Chinese backgrounds), this significantly decreases our pool of potential translators.

The obvious answer is to get more Australians without these foreign connections onboarded. It may come as little surprise, however, that Australians of a non-Chinese background who speak fluent Mandarin are few and far between. In fact, it's estimated that there are only about 130 non-Chinese Australians who speak Mandarin well-enough to conduct normal work purposes. This is a miniscule amount which should be at the attention of our national security agencies, and arguably already is.

When asked during a 2020 Parliamentary enquiry whether there's sufficient Mandarin language capability in Australia, Director-General of Security for ASIO Mike Burgess stated that "finding people with the right language skills who can pass a security clearance will always be a problem for us". Whilst he's satisfied with Australia's current capabilities, he acknowledges that ASIO relies heavily on the learning and development of its employees and that language skills are "an ongoing focus for [ASIO]." Although ASIO (accounting for only one of Australia's six security agencies) has enough translators as it stands today, this may change. Where would things stand if actual warfare broke out, where intelligence was no longer used just for policy and back-door diplomatic conversations, but was needed to immediately inform military decision making and save civilian lives? Could we afford to wait just two days, or maybe even longer, for a translation?

To help remedy this problem, we could also attempt to increase the number of Australians without a Chinese background who speak Mandarin by encouraging Mandarin in schools. In recent years only 10 per cent of year 12 Mandarin students have been of non-Chinese heritage and offering them a different ATAR stream may increase uptake.

Whilst not every student will study to fluency, it would be much easier to upskill those already with six years of experience should the country enter warfare and need all the translators it can get.

We could also attempt to improve existing Artificial Intelligence (AI) translation capabilities. Most of us have used Google Translate at some point to gauge the meaning of words in a language we don't know. This AI system, along with most others, relies on the online database of currently existing translations to 'learn' how to translate from one language to another (for example, if the Canadian parliament publishes a press release in English and French, an AI can take on this translation for an example of how to translate between the two). Conveniently, there are plentiful Mandarin resources which have been translated into English, giving Google Translate an accuracy rate of 4.3 (out of six), whilst human translators scored an only marginally better 4.6. Whilst little information is available about Australia's use of AI in intelligence translation, it is acknowledged that automated translation will be increasingly relied upon as we gather increasingly large swathes of intelligence data. Whilst our systems right now are far from perfect, AI has huge potential to be able to translate, sort, and analyse data on a scale human translators and analysts simply cannot accomplish.

However, simply training mass numbers of Australians with no Chinese background or creating a perfect translator AI (if such a thing is possible) will ignore a vital aspect of translation — cultural understanding. To have a proper translation of intelligence we need to have a proper understanding of the culture in which that language is written. For example, in Australian English, the word 'mate' could refer to a close friend, an adversary, or a person who one cannot recall the name of. Taking the dictionary meaning of this word as 'a partner in marriage' or 'animal reproduction' could have disastrous (or at least extremely confusing) translation outcomes. This is again repeated by Burgess stating "it's not just the language that we need… cultural understanding is critically important."

Whilst you can take culture courses within Australia or teach an AI to substitute a few words for others, this simply cannot compare to human translators living in a country and learning its culture from within. When we block the vast majority of people who have lived in China from gaining security clearances (noting the necessity for a checkable background and the difficulty that arises with checking backgrounds in China), we lose this much-needed cultural understanding.

In light of this, some have suggested overhauling the current security clearance process to make it easier for Chinese-Australians to gain security clearances. However, with some already slipping through the cracks of lower vetting levels, including a Department of Defence senior scientist engaging in side-dealings with the Chinese government's main missile manufacturer, it's questionable if national security agencies would be open to changing the supposedly water-tight Positive Vetting process.

A mixed approach will likely be necessary. It's unlikely that those who have recently immigrated from China, or who retain close connections to political actors within China, will ever be allowed access to intelligence. However, our intelligence agencies may be more willing to accept second, or even third, generation citizens who were raised in Australia but maintain some family connections in China. These applicants would maintain some level of cultural understanding, whilst being less of a perceived threat than others. For Australian speakers, we could also waive the checkable background requirement for short-to-medium term stays in China (for instance, under two years) if the applicant has been home long enough to determine they haven't maintained any risky connections. This would allow Australian speakers to gain some cultural understanding whilst keeping security risks to a minimum. Meanwhile, AI could be used to churn through raw intelligence and highlight anything of significance, which could then be passed on to human translators to conduct a proper culturally-sensitive translation.

Going back nearly twenty years, the intelligence that the NSA collected on 10 September 2001 likely couldn't have stopped the next day's attacks singlehandedly, even if it was translated in time. But this still goes to show that no matter how good national security agencies are at collecting intelligence, it's not worth much unless we have enough translators to churn through it. As China continues to grow more aggressive and the world continues to destabilise, Australia must acknowledge that its language barrier will become an increasingly gaping hole in national security, and others will be aware of it. Two decades ago, a two-day delay in translation probably wasn't what cost nearly 3000 lives, but it so easily could have been. Does Australia really want to take that risk?

Jessie is a fourth year Law and International Relations student at the University of Queensland who is passionate about the changing nature of Defence and National Security.

TECH TALENT IS KEY TO AUSTRALIA'S NATIONAL INTEREST

Jennifer Jackett,
Australian National University

Industrial revolutions aren't just paradigm shifts that people experience — people create them. Through imagination and ambition people set a vision and drive innovation.

With the fourth industrial revolution now unfolding, people are responsible for the designs, algorithms, and values embedded in new technologies from artificial intelligence to synthetic biology, and robotics. These people include data scientists, software engineers, programmers, and product managers, to name a few.

How effectively countries can mobilise strong technology workforces will determine their capacity to shape and benefit from these new technologies. Geopolitically, the dominant tech powers will attain economic, political, and military power and be better placed to secure their strategic interests and in line with their values.

Australia's tech talent crunch means we are falling short in one of our greatest assets — our people — to secure our interests in this digital age.

The cost of tech workers in Australia has increased by around 30 per cent in the past year.[1] This is the result of rapid digital transformation during the pandemic, border closures, and increases in workforce demands to support a global tech industry projected to total $4.1 trillion USD this year, up 8.4 per cent from 2020.[2] With all countries forecast to have skilled worker deficits by 2030, except for India,[3] the 'war of talent' is only likely to heat up as companies scramble for the world's best and brightest.

Momentum is building among policymakers and business to address this challenge. The government's recent Digital Economy Strategy includes $1.2 billion in investments across skills, emerging technologies, and government services to support Australia to become a leading digital economy and society by 2030. The recently formed Tech Council of Australia adds a powerful voice to advocate for the policy settings that can grow Australia's $167 billion tech sector.

While Australia's tech talent is rightly viewed as critical to Australia's economic prosperity and social wellbeing, there are growing strategic and national security imperatives to build this workforce. Tech talent is a critical factor in the ability of the US and its partners — including Australia — to maintain global technology leadership in response to China's ambitions, investments, and progress towards becoming a high-tech power by the middle of this century. Talent is central to continuing to develop cutting-edge civilian and military capabilities, growing companies and market share, and maintaining influence in international standard setting and technology governance organisations. Each of these has implications for military might, economic power, and global influence. The stakes couldn't be higher, as I argue elsewhere.[4]

In this era of techpolitik, the question becomes how Australia can practically build on existing plans to grow Australian talent to protect its interests in affordable, reliable, resilient, and secure technologies?

First, Australia is likely to maximise its returns by leaning into its tech strengths, especially in areas with industry-changing impacts, such as quantum computing, fintech, biotech, agritech, and clean energy. Rapidly scaling up initiatives to fund tech research and support commercialisation, such as establishing a national security strategic investment fund akin to the UK model,[5] would strengthen the development of a dual-use (military and civilian) tech ecosystem, with our military and national security community and those of our partners providing a market for such technologies. This could also support sovereign capabilities where they are needed.

Secondly, a long-term, nation-building agenda is needed to build the skills pipeline to support the needs of governments and businesses alike. A multi-decadal tech nation action plan encompassing schools, universities, business, and governments could focus on mentoring, internships, and training to strengthen pathways into, and advancement within, the tech sector. This should double down on initiatives to improve representation of women in STEM, and diversity initiatives more broadly. The plan should also recognise and support the range of other

occupations necessary to designing our tech future, like social scientists, ethicists, and philosophers.

Lastly, Australia has many shared interests with major tech players like the US, Japan, South Korea, Germany, and India, despite our distinct industrial bases. Notwithstanding companies in these countries are competing for talent, for high priority tech initiatives, agreements could be struck to use talent as a shared resource which countries could facilitate access to via multicountry talent program. The 'Quad' grouping of Australia, Japan, India, and the US could provide one forum to test a such an idea, for example, to support joint research initiatives under their Critical and Emerging Technology Working Group.

Ultimately, Australia's tech talent should be viewed as a national capability that supports economic prosperity and social wellbeing, and geopolitical and security interests. As a new technological revolution unfolds, the tech talent pipeline will underlie Australia's capacity to be a shaper and maker of this new era in line with our interests and realise our potential as an innovation nation.

Jennifer Jackett is a Senior Adviser in the Department of the Prime Minister and Cabinet in the Australian Government. She has also served in the Department of Defence and Office of National Intelligence and has experience advising government on a range of issues, including critical infrastructure, foreign interference, counterterrorism, international defence engagement, and defence capability development.

WHY AUSTRALIA CAN PLAY A LEADERSHIP ROLE ON CYBER SECURITY ISSUES IN THE QUAD

Daniel Phelan,
Monash University

Australia's thought leadership on cyber security issues presents a strong foundation for it to champion cyber cooperation as part of the Quadrilateral Security Dialogue (Quad) between Australia, the United States, Japan, and India. The Quad is in a position to engage with partners in the region, to address these shared challenges around cyber security, through a 'Quad Plus' arrangement utilising Pacific and Southeast Asian partners would help promote this engagement. Whilst, ensuring Australia and its allies can promote effective and positive cyber norms, alongside the defence of critical infrastructure assets in the region from cyber risks and attacks.

The Quad nations first collaboration as a grouping was as the 'Tsunami Core Group' in response to the Indian Ocean Tsunamis in December 2004 . This promotion of the Quad after 2004 was ultimately ill-fated and brushed aside, as leaders became wary of disrupting their bilateral relations with China. Subsequent Quad meetings planned in 2007 were cancelled due to Chinese objections to the purpose of a Quadrilateral Security Dialogue and limited momentum amongst Quad states to focus on the dialogue over other multilateral engagements such as the 'six-party talks'

Discussions among Quad nations re-emerged alongside the 2017 ASEAN Plus meeting. Leaders met to sketch a new path ahead for the dialogue with the aim of building resilience in the Indo-Pacific amid an increasingly uncertain geostrategic environment. The re-emergence in 2017 ultimately established the goals of the dialogue – the promotion of democracy, a rules-based international order, and a free and open Indo-Pacific coming alongside being a more general force for global good. It has since continued to evolve into a grouping which seeks to promote a more equitable balance of power in the region. By 2021, the group's momentum was quickly building, with leaders meeting virtually in March and at the first physical leader-level summit in September. Quad leaders again promoted its focus as a dialogue to ensure a free and open Indo-Pacific and reaffirmed the importance of a cyber-centric approach to the Quad. Leaders emphasised building trust, integrity, and resilience in critical technology supply chains, through building cyber norms and protecting critical infrastructure . Consistent with the recent Quad leaders' statement, cyber security cooperation and securing infrastructure in the region into the future aligns with the Quad's growing agenda.

Cyber security issues are at the forefront of the agenda for many states in the region and ever-present amongst Quad states, in response to the ever-increasing occurrence of cyber attacks. Australia faces self-reported losses from cyber crime totalling $33 billion , much of this affecting government entities, alongside one quarter of cyber security incidents impacting Australia's critical infrastructure. The United States faces similar issues, with attackers often targeting telecommunications providers, alongside American companies operating abroad . In September 2021, Japan's Internal Affairs and Communication Ministry announced attacks on its critical infrastructure were increasing and in a new drafted strategy, for the first time named North Korea, China, and Russia as cyber security threat actors attributive to many of these attacks. India also reported a range of cyber attacks affecting its healthcare industry, often stealing healthcare records, and shutting down health systems.

More broadly in the cyber landscape of the region, Taiwan faces 20 to 40 million cyber attacks per month, while Cambodia has also reported the hijacking of key supply chain infrastructure and its foreign ministry by attackers from within China . In response to these threats, Singapore and Taiwan have already broadened their focus on cyber security. Taiwan's "Cyber Warfare Branch" has become the first independent military cyber command in the world . While Singapore is investing $1 billion over the period from 2020 to 2023 to improve cyber security and data security capabilities, as well as establishing the ASEAN-Singapore Cybersecurity Centre of Excellence.

Malicious cyber activity may disrupt health facilities, electrical grids, and food supply chains, presenting dire implications for the stability of regional states. For states in the South Pacific already feeling the impacts climate change, cyber attacks to critical supply chain infrastructure would create an additional source of insecurity for which their governments are unlikely to have the capability to respond. A continued lack of investment into cyber security will drastically deepen the impact and regularity of such attacks launched by various state and non-state actors if vulnerabilities remain unaddressed.

The scale and scope of cyber threats in the Indo-Pacific illustrates the need for collaboration among like-minded partners. The Quad is well placed to take the reins and play a regional leadership role in supporting cooperation with a wider range of partners. As a grouping focused on policy coordination, the Quad can quickly respond to cyber attacks in a collaborative manner, by bringing not only Quad members, but also enabling future 'Quad Plus' dialogues with Indo-Pacific states such as Vietnam. Vietnam has reacted positively to the Quad as a dialogue if it can "ensure peace and stability in the region" but would oppose the formation of a military alliance. Other states such as Singapore also believe that the Quad's ability to promote rules-based norms can help ensure an equitably balanced region. A Quad which collaborates with ASEAN states will bolster its ability to respond and protect against state or criminal actors attempting to exploit cyber-enabled systems in the region, whilst continually bolstering the Quad's interests for greater cyber standards in the region.

Digital infrastructure holds a fundamental aspect of approaches to cybersecurity, acting as the building blocks to a resilient and efficient cyber network. There are a range of dynamics at play that can impact the potential vulnerability of cyber-enabled systems in the region.

China has recently expanded its investment in the Indo-Pacific region through its digital silk road policy, building 5G networks and data centres in the region. Aligning with China's Belt and Road Initiative, seeking to shape the regions digital infrastructure according to Chinese interests and standards, whilst benefitting Chinese state-owned enterprises. Meanwhile, the United States digital connectivity and cybersecurity partnership approach aims to promote free, open, and secure Internet in the Pacific, correlating with the goals of the Quad, rather than building their own 'franchising style' infrastructure and capabilities.

These investments aim to fill the gap in digital infrastructure, which is much needed to ensure states in the region do not fall too far behind. Currently less than 15 per cent of the Asia-Pacific region has access to broadband, equating to two billion people in the whole Asian region. This lack of digital access disproportionately affects low-income populations and women in these areas, and this contributes to the limited access to quality-of-life improvements and economic opportunities in the increasing digital age we live in. Addressing these issues of lacking digital infrastructure would boost tech literacy and encourage greater investments into deeper cyber capabilities throughout the Indo-Pacific, whilst also protecting critical infrastructure in the region. The importance of bolstering infrastructure, particularly in terms of improving digital connectivity is extremely important for future growth and development and would deliver more resilient cyber-enabled systems in the Indo-Pacific region.

The Quad's alignment with some of the region's major powers allows it to be at the forefront to ensure the protection of digital infrastructure in the region. The Quad can contribute to cyber security in the Indo-Pacific through the establishment of a cyber stability board. This could develop protection and resilience in responding to cyber threats. Creating greater resilience and tailoring cyber offensive capabilities are important to gaining asymmetrical cyber advantages. Furthermore, a Quad cyber stability board would have greater capability to develop practical counter-hybrid approaches to cyber threats, alongside the capabilities of limiting any consequences from cyber attacks. This is because of the Quad's potential to effectively navigate partnerships in the region and the existent technical architecture and resources these states possess.

One of the predominant aims of the Quad should be to work with existing governance arrangements in the region, such as the Association of South-East Asian Nations (ASEAN) and the Pacific Islands Forum. The Boe Declaration is progress Pacific states have already taken, enshrining the importance of cyber security to "maximise protection and opportunities for Pacific infrastructure and people" . These approaches should be expanded and honed through the Quad to promote the importance of cyber issues in the region and develop greater resilience to cyberattacks from state and non-state actors in the region.

Australia has a key role to play in the Quad. It is also uniquely placed to advocate for the interests of not only itself, but its neighbours throughout the Pacific Islands. Australia's own cyber security centre is a member of the Pacific Cybersecurity Operation Network (PaCSON). PaCSON aims to improve collaboration and work closely with organisations in the region, mirroring Australia's interests as outlined in the Department of Foreign Affairs Cyber Cooperation program in the Pacific. Australia's focus on empowering collaboration and information sharing through the Quad is an important component of regional cybersecurity, as it creates greater connection and collaboration to respond to and analyse cyber incidents.

Australia can spearhead the Quad's approach to cyber security developments in the Pacific. Emphasising a multilateral approach will help build resilience to malicious cyber activity and encourage collaboration through information sharing and secure digital infrastructure.

Daniel is a fourth-year undergraduate student at Monash University studying International Relations, Computer Networks and Security & Chinese (Mandarin) Studies.

WHY AUSTRALIA MUST IMPROVE ITS CYBER SPACE DEFENSIVE CAPABILITIES

Stephan Robin,
University of Adelaide

For much of Australia's history, distance has been its greatest defence from foreign powers. But in a world where nations use cyber warfare to undermine strategic advantages, distance may now pose a vulnerability to Australian security as we develop a reliance on increasingly compromised satellite technology.

Australia finds itself grappling with these new risks at a time of heightened geopolitical tension. Recent years have shattered the post-Cold War dream of cooperation and strategic restraint in a variety of domains, but especially in space. The Australian Government's ambition to develop sovereign space capabilities coincides with many other nations turning away from international cooperation and towards national power projection. With the United States joining China and Russia in having a military branch dedicated to space combat, and India, France, Japan, Canada, and the United Kingdom developing similar programs, we are clearly entering a new chapter in space geopolitics.

This reality is seemingly not lost on the Australian Government. Following the formation of a domestic space agency in 2018, in May of this year the Department of Defence announced the establishment of a space division within the Air Force. The stated purpose of the division is to protect Australian space interests through orbital domain awareness. However, Defence's decision to conduct a Space Domain Review, due for completion by the end of 2021, suggests that what exact capabilities Australia needs to operate in this area, is still an open question.

Counterspace technologies typically fall into one of four categories — kinetic, electromagnetic, electronic, and cyber. The first three are reasonably conventional and involve well-established technologies, to the point where in 2015, the United States was unintentionally jamming its own communication satellites an average of once every two days. Cyber attacks on the other hand are particularly singular in the threat they pose, and in the case of satellites, are capable of simultaneously exploiting two distinct vulnerabilities. Namely, Australia's unique satellite dependence and the difficulty in attributing cyber attacks. Australia is utterly dependent on satellites for many of its day-to-day operations, especially given the country's large size, which necessitates satellite coverage to monitor and communicate over vast distances. These include supplying key military intelligence, connecting Australia's remote interior, underpinning economic productivity, and improving water and resource management. There are few sectors in Australia that would be unaffected by even a temporary disruption to our satellite network.

Compared to other anti-satellite technology, cyber attacks are more readily deployable with less resource investment, and they often avoid international fallout by allowing states to maintain deniability. Particularly in space, the difficulty in physically examining satellites compounds the issue of deniability by allowing a cyber attack to be masked as an innocent system fault or a natural collision with space debris.

Cyber attacks also have the capability to target an entire network at once, as opposed to a single satellite. For example, the 2017 Petya malware attack on accounting software used in Ukraine rapidly spread throughout the country's digital network, affecting most of the nation's critical infrastructure. For the duration of the attack government ministries were deprived of computer access, banks were unable to facilitate commercial transactions and transportation systems were compromised. Even radiation monitoring systems at the Chernobyl nuclear site were disabled and operators were forced to revert to manual radiation monitoring. For these reasons, former chief of The Australian National University's Cyber Institute Lesley Seebeck described cyber attacks as 'the most immediate threat to our critical infrastructure and the biggest threat to our government and security'. The common function of satellites as communication platforms makes them even more susceptible to being used for these sort of system-wide attacks.

And Australia's reliance on satellite technology is only growing. For example, next year, Queensland based company Fireball will begin the launch of their bushfire detection constellation of satellites, capable of detecting fires anywhere in Australia mere minutes after ignition. This would allow firefighters to quickly extinguish a blaze before it turns into the sort of devastating bushfires that were seen in the 2019-2020 Black Summer that killed 479 people and had a projected national cost

of nearly $100 billion. As Australian authorities grow used to the early warning provided by such technologies, a well-timed cyber attack that disables these satellites, even for a few minutes, would completely undermine Australia's ability to prevent a repeat of these wildfires. This could cause tremendous environmental, economic, and societal harm while allowing the belligerent state to avoid international retaliation.

Another example of Australia's future satellite dependence is our growing use of satellite data to optimise supply chains. While Australian supply chains have held up reasonably well throughout the pandemic, the experience of harder-hit countries have laid bare the consequences of serious disruptions. The ability of satellites to obtain highly-detailed, real-time information at a world-wide scale is already being proposed as a way to build resilience into the Australian and global economy. Satellites with hyperspectral cameras could be used to predict agricultural output months in advance of harvest, and high-resolution cameras would allow for land and sea freight operators to minimise route congestion and inefficiencies of transport networks. The value of satellite data will likely see satellites assume a more significant role in the day-to-day Australian productivity. While there is significant potential gain here, this will also expose the Australian economy to malicious cyber attacks, while still allowing hostile actors to maintain the veil of anonymity and deniability that makes retaliation nearly impossible.

What is most worrying is that cyber attacks targeting satellites have occurred before. The first such attack was in 2007, when the Tamil Tigers separatist group hijacked a United States communications satellite to broadcast ethno-nationalist propaganda. Between 2007 and 2009 there were multiple attacks against NASA satellites. Twice in 2008, hackers believed to be connected with Beijing bypassed the security systems of the Terra NASA climate research satellite, and in both cases were in a position to issue commands and cause permanent damage to the satellite. Though the hackers did not send any instructions to the satellite, American space assets were firmly under the control of foreign actors for several minutes.

Cyber warfare has grown more nuanced and prolific since 2008, but there have been few reports of similar incidents of satellite cyber seizure. While this could be interpreted as indicating a diminishing cyber threat to satellites, it could also suggest that the technology is still being developed, just with more discretion. The repeated hijacking of the Terra satellite without any accompanying demands of ransom or wanton destruction implies an actor looking at developing and testing their future capabilities rather than securing an immediate material advantage. And given recent heightened global tensions coupled with a clear preference for covert hostilities, this interpretation seems far more likely. Despite the limited public record of these cyberattacks since 2009, as recently as 2017 a senior American military official reportedly stated that cyberattacks are the most pressing counter-space threat to the existing and future development of space capabilities.

The five operational domains of warfare are not equal. Space encompasses the land, sea, and air, and cyber permeates them all. To protect Australia and its national interests, defensive space capabilities are needed. Although Australia is a few years behind in this realisation, it is a reassuring sign that a dedicated space division within defence is being formed. But to ensure the reliable operation of Australia's current and future space assets, there must be an awareness of the importance of proactively extending our cyber security concerns beyond our atmosphere.

Stephan Robin is a final year undergraduate studying a Bachelor of Arts and Bachelor of Science at the University of Adelaide. He is currently interning with the Office of the South Australian Chief Entrepreneur and assisting with research at the Institute for Photonics and Advanced Sensing.

A NEW AGENDA FOR GLOBAL ARMS CONTROL: BANNING KINETIC ENERGY ANTI-SATELLITE WEAPONS

Cosmo Jones,
Australian National University

During escalating geopolitical tensions over ownership of an island in the South China Sea, several missiles are launched from a submarine lurking deep below the surface. Never to return to earth, their target is a satellite orbiting hundreds of kilometres above. Moments later, another barrage is fired from a nearby island. They too hurtle towards an orbiting satellite. They all hit their targets. These are the firsts shots fired in anger in a conflict between major powers.

The satellites are destroyed. They break up into thousands of pieces which then begin their own uncontrollable orbit of the earth, forming thousands of wrecking balls travelling at roughly 25,000 km/h. They hit and destroy another satellite, then another, creating more unstoppable debris. Within several weeks, collisional cascading of debris has begun. There is now so much space debris in orbit that transit to and from earth is virtually impossible. Within months, all existing satellites will be threatened.

Without satellites, global telecommunications, transport, power, and computer systems are severely disrupted. Civil aviation grinds to a halt. We can no longer forecast the weather effectively. Financial institutions struggle to stay online. Intelligence gathering is interrupted. High-end 'smart' weapons systems from missile defence to drones lose their 'smart.' Future manned space missions are now suicidally dangerous and unmanned missions become prohibitively risky and therefore expensive, leaving the world stranded on Earth. Worst of all is the loss of Global Positioning Systems, so anyone born after the advent of smartphones is lost because they can't read a map.

This apocalyptic scenario is worryingly conceivable. Modern militaries are heavily reliant on satellites for a whole range of tasks, from simple communication between units to complex targeting systems and everything in between. Satellites are the 'modern' in modern militaries. This makes them valuable targets.

Missiles that can target those satellites are called 'kinetic energy anti-satellite weapons', KE-ASAT for short. They are purpose-built to collide with — and destroy — satellites. These weapons have the potential to cripple an adversary's battlefield operations and they could be the first shots fired in a conflict between major powers.

Science fiction?

The United States, Russia, China, and India have all successfully tested KE-ASAT weapons, and Iran and Israel have the capabilities to quickly develop them.   These tests have already produced a dangerous amount of deadly space debris. In 2007, China tested a KE-ASAT missile on one of its old weather satellites. The test produced over 3300 pieces of trackable debris – a single piece the size of a speck of paint can destroy a satellite. Most of the debris created by this test will stay in orbit for centuries to come. This is not science fiction.

It is important to note here that we don't have tested methods of removing space debris. In 2025, ClearSpace-1 will launch. This will be the first attempt to remove a piece of debris from orbit. With luck this will be successful and could help to promote a market for de-cluttering Earth's orbit, but science is not there yet, and the Earth's orbit is already dangerously close to a tipping point in which it becomes unusable due to cascading collisions of space debris. This tipping point is known as 'Kessler Syndrome', and we are a few bad decisions away from putting his theory to the test.

The time is ripe for an international agreement

The stakes are higher than ever, and they will continue to rise, as will the number of stakeholders. It was 1959 when the United States first successfully tested a KE-ASAT weapon, at that time the United States and the Soviet Union were the only powers to have satellites in orbit (four in total). As of today, there are 4,084 satellites in orbit operated by 92 different countries and private companies. The global space economy is worth an estimated $350 billion.

At the G7 Leaders' Summit in Cornwall in June of this year, delegates from Canada, France, Germany, Italy, Japan, the United States and the

United Kingdom published a joint statement committing to "the safe and sustainable use of space to support humanity's ambitions now and in the future." The statement explicitly recognised space debris as a global challenge.

The United Nations General Assembly tabled a Resolution in December 2020 titled 'The Prevention of an Arms Race in Outer Space' The Resolution emphasised "the importance of maintaining outer space as a peaceful, safe, stable, secure and sustainable environment for the benefit of all". 25 spacefaring countries wrote responses to this resolution, they were presented to the Assembly in July 2021 — only a month after the G7 Leaders' Summit. All four countries that have demonstrated KE-ASAT capabilities responded. Their responses reveal important conclusions about the prospects of an international KE-ASAT weapons ban.

China expressed explicit support for an international legally binding arms control treaty in its response. China's response states, "All countries should support prevention of the placement of weapons in outer space and the threat or use of force anywhere against outer space objects through legally binding measures." Further, China indirectly challenged the United States by stating, "Whether a country has the political will to participate in such a negotiation is the touchstone for its sincerity in terms of behaving responsibly."

In similar language, Russia also expressed explicit support for a binding arms control agreement. Its response states, "the threat or use of force against and with the use of space objects should be prohibited" and "The United Nations should advocate reaching appropriate, closely monitored and legally binding multilateral agreements as soon as possible through negotiations." However in 2020, Russia allegedly tested a space-based KE-ASAT weapon, casting doubts on their commitments.

India's response was more lukewarm. It didn't explicitly support a binding agreement though it expressed a desire to see space remain an "operationally stable and safe environment that is maintained for peaceful purposes in the interest of all countries, without discrimination of any kind and with due regard for the principle of equity." India was the latest country to officially test a KE-ASAT weapon in 2019.

The United States response is telling and suggests it may be the most stubborn obstacle to an agreement. In contrast to Russia and China it advocates for "voluntary, non-legally binding norms, rules and principles of responsible state behaviour with regard to outer space." Further that, "States could consider elaborating best practices or responsible behaviours that avoid simulating or testing anti-satellite weapons in the direction of, or in close proximity to, another state's satellite."

This is no surprise, the United States has long since avoided committing to international agreements and treaties which may get in the way of its sovereign decision-making (while often strongly advocating for them internationally). Also, the United States is the only country so far to have to have declared space a 'warfighting domain'. In 2020 the Department of Defence (DoD) published the world's first doctrine for warfare in space declaring, "The Department will grow its space power capacity over the next 10 years to ensure space superiority and secure the nation's vital interests." It is clear the United States has no intention to reduce its space warfare capabilities and is instead looking to cement its dominance in the space domain while promoting voluntary norms to guide activity in space.

Where to from here?

Where does this leave us on a KE-ASAT ban? China and Russia have already demonstrated a willingness to engage in diplomatic talks on this issue with their proposed treaty to ban the use of force in outer space. But their proposal doesn't have a mechanism for verifying or enforcing compliance. Meanwhile, they continue to develop their KE-ASAT capabilities. India has avoided expressing support for a legally binding agreement and tested a KE-ASAT weapon as recently as 2019. The United States has advocated for the development of non-binding norms to constrain state behaviour while signalling it aims to achieve military dominance in the space domain.

Middle powers like Australia, Japan, the United Kingdom, Italy, Germany, France, and Canada should continue to push this issue in high-profile forums like the General Assembly and in smaller groupings like North Atlantic Treaty Organization and the Quadrilateral Security Dialogue. Specifically, they should encourage the Biden administration to lead the charge on pursuing a multilateral agreement with China, Russia, and India that have demonstrated KE-ASAT capabilities.

The agreement should be limited in scope to encourage cooperation. The historical precedent of Cold War era arms treaties between the United States and the Soviet Union suggest that a limited agreement is more likely to succeed. It should specifically target KE- ASAT weapons which have the potential to cause uncontrollable space debris. Countries party to the agreement could retain the option of developing and deploying non-kinetic ASAT weapons that don't produce space debris — as they already are.

Australia should appoint a thematic Ambassador for Space Affairs within the Department of Foreign Affairs and Trade to lead the diplomatic effort. This role should be modelled on the Ambassador for Cyber Affairs and Critical Technology position, currently held by Dr Tobias Feakin.

It is not only in Australia's national interest for such an agreement to succeed. It is in humanity's interest.

Cosmo Jones holds a Masters of National Security Policy from The Australian National University National Security College.

AUSTRALIA IS NOT PREPARED FOR AN INFODEMIC

Abigail Masters,
RMIT

The lack of attention given to media literacy and misinformation by government stakeholders may grow to be one of the biggest national security failures of the 21st Century. Australia is currently playing catch up to address strategic cyber-threats but has failed to meaningfully mitigate the danger of misinformation in Australian digital spaces. Over the last 20 years, Australia has witnessed a rapid development in communications technology. From the introduction of Web 2.0, the creation of social media giants such as Facebook, to the increasing likelihood of quantum computer systems, the evolution of the digital space is something to behold. Thanks to these technologies, the average Australian has more access to knowledge than at any other point in history. But despite these developments over the last twenty years, it is only recently that cyber security has taken a strong foothold in national security strategy.

Australia's 2020 Cyber Security Strategy announced an investment of $1.67 billion AUD over the next decade into "creating a more secure online world for Australians, their businesses and the essential services upon which we all depend". What was glaringly absent was any mention of information manipulation as a threat in the cyberscape. Its omission can be attributed to Australia's perception of cyber security, which defines cyber security by "measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them" This view is simply not enough in today's digital landscape. Cyber warfare and threats go much further than ransomware, phishing, and malware attacks and are now moving into targeted conspiracy and misinformation campaigns.

Warning bells have been ringing for quite some time about the threat of malicious information campaigns. In 2019, Chief of the Defence Forces Angus Campbell stressed that Western societies are witnessing a "modernised version of political warfare", a time where subversion and disruption tactics are increasingly being used to undermine societies. These grey zone operations are allowed to thrive because of traditional and outdated perceptions of warfare. Australia is no longer at a crossroads when it comes to security. Rather, recent disinformation campaigns and the prevalence of conspiracy theories are only the surface of a variety of interconnected security challenges that will only evolve in coming years.

While information campaigns may not have the same immediately explicit effects as cyber attacks do on infrastructure, the consequences remain equally insidious. In times of great global crisis, people need support, validation, and control. Conspiracy theories exploit these needs, prey on the fears of individuals and exploit the human desire to protect. In fact, they amplify a multitude of threats. Studies into the psychology behind mass belief in conspiracy theories is currently lacking, but current research suggest several motivations. A key finding is that people are motivated to turn to conspiracy theories when they feel anxious and powerless. These theories can also make people feel like they are protecting themselves from a threat that is cheating them. Such responses have been acutely visible throughout the COVID-19 pandemic.

Every Australian is now familiar with the mass lockdowns implemented to quash the consequences of major COVID-19 outbreaks. A by-product of this is the way that ordinary people's lives have been uprooted, often with financial and psychological implications. An alternative would have been to 'let the virus rip' — the consequences of which would not only lead to thousands of deaths from the virus itself but also thousands more from a collapsed health system.

The underlying issue with a threat like the pandemic, in terms of public perception, is that it isn't always possible to 'see' an illness. You cannot see a virus passed from one person to another. There is no sound of artillery fire, there are no bombers flying overhead. The double-edged sword of managing the spread to the point where most healthy people aren't immediately impacted is that for many not directly exposed, it can seem like the threat does not exist.

Meanwhile, COVID-19 conspiracy theories have run rampant online in Australian digital spaces and globally. These include anti-vaccination

misinformation, beliefs that COVID-19 was caused by 5G and views that lockdowns have been an effort by the government to control and subjugate Australian communities. Director General of ASIO Mike Burgess flagged COVID-19 and conspiracies in is second annual threat assessment. Among other challenges that were brought about COVID-19 he stated that "extreme right-wing propaganda used COVID to portray governments as oppressors, and globalisation, multiculturalism and democracy as flawed and failing". Here, a picture begins to be painted about the local nature of misinformation.

Concerningly, these campaigns have moved beyond online spaces and into the streets, manifesting into 'freedom' protests across the country. The world is beginning to witness the physical danger of conspiracy theories, visible in the storming of the United States Capitol building as well as white theories of genocide , which contributed to the Christchurch Mosque shooting in 2019. Aside from the freedom protests that have occurred sporadically across the country during the pandemic, Australia is yet to have a major national security incident fuelled by conspiracy theories. But this does not mean that it will not occur.

As a result of COVID-19, Australians are spending more time than ever before online, and efforts by social media platforms have been insufficient to minimise the spread of misinformation and conspiracy theories. In the 2021 study "COVID-19 Misinformation Trends in Australia: Prospective Longitudinal National Survey" researchers found that at the beginning of public health measures in Australia, there was a stronger agreement with misinformation from young males who held lower levels of education and spoke languages other than English at home. While this is only one study that occurred very early on in the pandemic, it shows an institutional failure in addressing intersectional factors that influence information comprehension and interpretation of media messages.

The risk of misinformation and conspiracy theories moves far beyond immediate health consequences. The decline of trust in government, science, and facts leads to a very real erosion of democracy and lays the perfect foundation for foreign interference, radicalisation, and disregard of the rule of law. Social media trends are already being studied and it evident that states are attempting to wield online spaces for political gain. A 2020 report by the Australian Strategic Policy Institute emphasised that "Chinese state's efforts to contest the information domain are supported by coordinated, although not necessarily inauthentic, pro-China patriotic trolling.". It would be naïve to assume that China is the only state doing so.

Australian digital literacy programs have also come too late for many populations interacting online. The Australian E-Safety Commission has a primary focus on protecting children and the elderly, while vast demographics in between are left out. Additionally, the E-Safety commission tends to focus heavily on scams and exploitation. These are important issues, but a new focus on the dangers of misinformation and prevention of radicalisation needs to be seriously considered in future communication to the public. Further, COVID-19 has highlighted the need for an overhaul in how governments convey information to our many linguistically diverse communities.

The digital revolution and ease of access to information have fundamentally re-shaped the way we live. But policymakers cannot continue only to adapt to potential threats — they must be proactive and focus on their prevention. With the sentiments of Major Angus Campbell quoting Leon Trotsky, "you may not be interested in war, but war is interested in you."

Abigail Masters is a final year Bachelor of International Studies student at RMIT University.

HOW CAN AUSTRALIA RESPOND TO CHINA'S DISINFORMATION CAMPAIGN?

Paul Sigar,
University of Adelaide

Democracies around the world are facing the growing challenge of cyber-enabled foreign influence and interference. In Australia, foreign interference has scaled to an 'unprecedented' level in recent years, posing an 'existential threat' greater than terrorism. Although Australia did not experience any foreign interference or malicious cyber activities that affected the integrity of its 2019 federal elections, this may change in the coming years. Australia can expect disinformation campaigns perpetrated by Chinese state actors, similar to those that target Chinese diaspora in North America, to reach its shores — only more sophisticated and covert.

This proposition is based on two observations. The COVID-19 pandemic has highlighted the susceptibility of the culturally and linguistically diverse communities in Australia to disinformation, misinformation, and false narratives. Overt intentions by the Chinese Communist Party (CCP) to weaponise the Chinese diaspora to advance its ambitions should concern Australia. Further, with rhetoric about China turning into a domestic political debate, this discourse is only becoming more politicised and polarised, and will likely dominate Australia's policy debate in the upcoming elections. This environment creates fertile ground for foreign interference.

The rising tension between Australia and China also increases Chinese incentive to interfere with Australia's democratic processes. There is no indication that China has a preferred prime ministerial candidate or political party, and it is very probable it never will. In this context, rather than influencing Australia's democratic processes to install a preferred candidate or party, a foreign influence and interference operation by the CCP is more likely aimed at discrediting China's critics in Canberra, deliberately polarising political discourse on topical issues, trivialising national security concerns by accusing Australia of paranoia, and sowing discord on matters involving Australia's strategic interests such as the AUKUS alliance or the status of Taiwan.

A snippet of China's disinformation strategy

Disinformation is the deliberate dissemination of false information with the express purpose of causing harm. Disinformation operations can be carried out by inauthentic actors (such as trolls and bots) or authentic actors. The disinformation experiments by the CCP on the Hong Kong protests and the COVID-19 pandemic provide a prequel of what to expect. There are consistent themes throughout China's information warfare — the weaponising of current affairs to project Chinese strength, with the primary target being Chinese diaspora communities. Such disinformation campaigns also tend to entail elements of Chinese nationalism while sowing distrust in public and scientific institutions of its adversaries.

But how effective are China's disinformation campaigns?

It is unclear how successful China's disinformation campaigns have been. Measuring the 'success' of an information operation remains difficult because there is an element of human autonomy and decision-making capacity. Like the 2016 United States' presidential election, no one can definitively claim that Hillary Clinton would have won had it not been for Russian interference. The metric of success becomes even harder to measure when a disinformation campaign does not produce an immediate, observable outcome — such as the successful election of a preferred candidate — but has nevertheless resulted in the long-term ancillary harm. For example, while the perceivably more China-friendly Kuomintang failed to wrest power from the Democratic Progressive Party in Taiwan, the island is now more divided than it was pre-pandemic as a result of China's use of disinformation. So it is imperative that when formulating a policy approach, policymakers turn their mind to the foreseeable long-term ancillary harm that may arise, and not just the direct and immediate harm misinformation may cause.

How Australia should and should not respond

Disinformation campaigns, if conducted in collaboration with a foreign principal to harm Australia's national interests, may constitute an offence under Australia's latest foreign interference law. While the law can be a convenient tool to achieve a desired outcome, over-legislation is not always the answer. The law is not always swift and effective. Rather, the fight against disinformation constituting foreign interference should go further than the realm of law enforcement to active engagement that prioritises swift action.

Sun Tzu once remarked, "speed is the essence of war. Take advantage of the enemy's unpreparedness; travel by unexpected routes and strike [them] where [they] have not taken precaution." In the Australian national security context, the same principles apply to information warfare. The national security framework must prioritise speed, preparedness, and precaution or heightened alert.

When dealing with authentic actors, censorship, spreading counter-disinformation, and de-platforming, though convenient, should not be the first response. Instead, counter-disinformation strategies must be underpinned by underlying democratic principles. This is especially important for liberal democracies like Australia — it is what makes Australia different to authoritarian regimes like China. Here, Taiwan is a successful example of how a country can fight disinformation not just without resorting to censorship, but also being radically transparent. To quote Taiwan's Digital Minister, "anything around censorship is a nonstarter".

Whether through software or other means, Australia can implement mechanisms for swift detection and response to harmful manipulated information. An independent national fact-checking system that employs a double-blind review can be established, which should be transparent on how the vetting of fake news is conducted and include mandatory disclosure of funding interests. In Taiwan, the '2-2-2' strategy aims to counter disinformation by responding to any disinformation within 20 minutes with 200 words or less and with two images that prioritise 'humour over rumour'. This strategy is meant to communicate key information to the audience swiftly and succinctly.

But the real challenge for Australia is how to roll out counter-disinformation strategies without them being perceived as anti-China propaganda. Part of the solution is to continue supporting a robust media and a vibrant democracy. This means welcoming constructive debates, promoting a culture of transparency and accountability in government and in journalism, and most importantly, encouraging critical thinking in public discourse. The discourse on fake news and misinformation should be embedded in critical self-reflections. Critical thinking and self-reflection construct better epistemology — the understanding of knowledge and sense-making — which is a crucial component of a mature democracy. Discourse on fake news should focus on nuances of opinion, instead of merely presenting an alternative view or 'debunking' 'false information' with 'the facts'. Disproving fake news — even with the most accurate facts — rarely changes someone's views, and usually only leads to further polarisation. A healthy level of scepticism should be welcome, but equally, people should be encouraged to challenge their own thoughts and beliefs.

Any such efforts to counter disinformation must also include diaspora communities, and respect the nature and context of the vulnerability of such groups. Australia has tailored multilingual messages for COVID-19 related information, but a recent study shows that strong agreement with misinformation is more an issue of digital illiteracy and mistrust in public institutions than language barriers. To build public confidence in the body of expertise and public institutions, government communiqués must consistently prioritise key messages in a comprehensible and easily accessible manner.
An improved visibility and transparency may also alleviate distrust in public institutions. Among other things, the right to access information under the Freedom of Information Act can be an important tool to foster trust in public institutions.

There should also be greater public awareness around the issue of foreign interference to facilitate a whole-of-society approach to combat disinformation. At present, the discussions around foreign interference and other national security issues have yet to seep into the mainstream. Internet users should be better equipped and educated to detect misinformation and spot hallmarks of disinformation. An increased awareness creates a sense of agency and responsibility, which lays the groundwork for a resilient citizenry. In Taiwan, the growing civic tech community sets an example of digital democracy that is resilient to malign foreign actors.

It should also be acknowledged that the rise of xenophobia and distrust against Chinese-Australians does not help. The tone of the conversation around China-Australia relations needs to remain firmly objective, with criticisms clearly directed at the CCP, not people of Chinese descent. Consistent with Australia's national agenda of multiculturalism since 1978, civil societies and community leaders should initiate grassroot efforts to strengthen social cohesion, foster civic commitment and encourage political participation and activism among culturally and linguistically diverse communities.

Regardless of what policy response Australia opts to adopt, it must be evidence-based and evidence-led. To achieve this, think tanks need to continue working closely with the Australian Government to study the effectiveness and impacts of foreign disinformation operations, so that a more targeted measure can be taken.

It is also high time Australia's national security framework includes a visible emphasis on multiculturalism. Beyond the Canberra bubble, the general Australian public needs to know that the array of lived experiences, knowledge, and language skills represented by Australia's diverse communities is not only a rich source of intelligence, but also a lens to certain world views. A strong, diverse, and socially cohesive Australia is vital to Australia's security interests, particularly in responding to China's disinformation campaigns.

Paul Sigar is a Bachelor of Laws (Honours) graduate from the University of Adelaide and delegate with the Australian Crisis Simulation Summit 2021.

THE HUMAN BODY AS A NATIONAL SECURITY THREAT

Rebecca Banalaga,
Australian National University

If you're reading this, you're on the Internet. As such, you're likely to be a user of the Internet of Things (IoT) — the network of physical devices connected to the Internet. And our obsession with IoT is just getting started. In recent years, consumers, industry, and businesses alike have flocked to these smart devices for convenience, efficiency, and often just for fun. Researchers from McKinsey & Company found that in 2015, the potential economic impact of the IoT would equate to over $11 trillion each year to 2025.

But whilst the IoT brings us joy and efficiency to our daily lives, it also poses a significant number of vulnerabilities and concerns. From issues surrounding data to privacy, ethics, and legal complexities, we face many risks on the IoT. According to the World Economic Forum, these risks increase significantly when you merge the IoT with the human body. The Internet of Bodies (IoB) is an archetype of the IoT, connecting the Internet and Internet-connected devices to the human body. IoBs are technology that we voluntarily allow into our bodies, by ingesting, implanting, or wearing them. In doing this, we transform our bodies into the newest data discovery platform.

IoBs can be split into three generations — 'body external', 'body internal', and 'body embedded'. 'Body external' consists of wearable devices such as insulin pumps, Apple Watches, or Fitbits. 'Body internal' includes devices that are inserted into the human body to monitor or control various health aspects, including pacemakers, smart contact lenses, or cochlear implants. Finally, 'body embedded' describes technologies that merges the human body and technology together to a remote machine. An example is embedded radio-frequency identification microchips, such as those that bio-engineering company Biohax International introduced in Sweden, which enable employees to gain access to their work building without a swipe card or key.
As early as 1996, a prototype of an IoB was unveiled which enabled two humans to exchange business card information solely via a handshake. Since then, the number of devices that encompass IoB has grown significantly, and their benefits have been widely documented.

One example is the potential to identify whether a cancerous cell has begun to multiply in real time. It's no less than a miracle that this deluge of metadata can help healthcare services to monitor patients with closer accuracy than ever before, tracking them using geolocational data in case of an emergency, for example. But alas, like most other technologies, there are significant concerns too.

Increasingly on the news are stories of ransomware attacks on critical infrastructure assets or major industries, including the Colonial Pipeline, JBS Foods and, more recently, Accenture. We've seen the impact that cyber criminals can have on the security technology of multi-billion companies and assets, and that feeling of vulnerability and fear to be at the behest of another actor. But it's not only multinational companies at risk. Vulnerabilities can also affect the individuals themselves that house IoB devices.

In 2013, former United States Vice President Dick Cheney replaced his Wi-Fi-connected defibrillator with one without Wi-Fi capacity. He did this due to fears that a rogue cyber criminal would hack into the device and assassinate him by electric shock. Whilst this likely put Cheney's fears to bed, unfortunately there are also other ways that devices can be exploited without Wi-Fi. Cyber criminals can steal data through memory operations and Wi-Fi receivers. This was exactly what was experienced in the 2010 'Stuxnet' attack, in which USB-delivered malware was able to compromise nearly a fifth of Iran's nuclear centrifuges. Alternative methods also include radio waves, electromagnetic waves, the Global System for Mobile Communications network, and even heat sensors.

Although, a University of Texas academic, Professor Dean Sittig, says that there aren't many incentives for cyber criminals to attack a single medical device unless it's connected to a celebrity or someone of a notable or prestigious background. Still, being complacent and ignorant about information security can also present significant privacy and confidentiality concerns. In 2020, RAND Corporation researchers found that some IoB devices can track a human's sight, hearing, bodily functions, and even thoughts — and there's unresolved questions about who can access this data.

An IoB can enable an individual or group to monitor, extract or exploit data or records. Once an attacker is inside the device, they can steal private information, release malware into the system, disrupt operations, or even launch a ransomware attack. In a health setting, it could also be used to modify existing records and lead to incorrect prescriptions and dosages, or possibly prescribe deadly treatments using an inaccurate electronic health record system. It leaves future regulators, lawmakers, and policymakers with questions about privacy and legal concerns.

But some companies are slowly clocking onto the value of IoB data. In mid-2020, PC Mag reported that Microsoft patented an application to authorise bodily functions for mining cryptocurrency. In essence, the application enables responses such as body heat, fluids, or brain waves to generate validation in a blockchain system. The company envisaged, somewhat sinisterly, that they would reward users with digital currency for being monitored in such an invasive way. The data mining possibilities for companies and advertisers are truly endless.

There are also unresolved and imminent legal uncertainties and implications, with inconsistent legal decisions made already in IoB litigation. Writing for The Wall Street Journal, Professor Andrea Matwyshyn implies that regulators and the courts are just not ready for IoB devices. There are far-reaching concerns for regulation, contract law, and intellectual property at the very least, and they're yet to be fully explored.

It's also becoming clearer that these devices can garner unfair inequalities in those using IoB devices. Consequently, regulatory and legal concerns arise about how to handle potential discrimination and bias. For example, not many people give all that much thought to potential impacts on insurance.

There are questions about whether providers can deny cover based on an individual's poor health and lifestyle choices that they confirm through IoB data, as insurance companies can retrieve this diagnostic data and refine their assessment of a user using more accurate and statistical methods, aiming to calculate the risk associated with a user's lifestyle.

Also poorly understood are potentially adverse consequences on employment and job opportunities. Imagine an employer pays to obtain IoB data on a prospective employee. There is a chance that they may not like what they see. For example, they might consider the recruit to be reckless with their privacy decision-making, think they could pose a health risk to staff, or believe that it's too difficult to accommodate to the accessibility of a new arrival with an embedded IoB device.

For more strict working environments that already ban or discourage the use of electronic devices — such as certain government departments, contracting services, emerging technology industries, sensitive laboratories, or academic spaces — employers may not hire them as their device harbours the potential to damage, steal, track or interfere with equipment, assets, or information in the workplace. Another reason could be that their IoB's data is stored in another company's holdings, in the cloud, in a data centre, or in a country that they consider to be less than favourable.

IoB devices also present unfavourable ethical considerations. Researchers El-Khoury and Arikan seek to answer the questions around the balance between an increasingly appealing technological capability that improves wellbeing and healthcare, with the need for vital safety and individual autonomy. They also discuss how humans are progressively losing control over yet another seemingly innocuous device that presents complexities and widespread concerns over human choices.

With all these concerns, it's obvious that more needs to be done. Stakeholders who must be part of the solution include manufacturers of IoB devices, cloud service providers, health care organisations, governing bodies, unions, lobbying groups, insurers, end-users, and more. These groups all need to be on the same page to ensure that proposed mitigations can keep pace with changing legal landscapes and emerging technologies. At the same time, government needs to craft measured procedures and make considered decisions in response to these security concerns, and to tackle a growing list of evolving threats. On top of that, it's essential that basic cyber security training and education for health practitioners and medical students must be embedded into the medical curriculum. This will boost the awareness of health professionals and provide more informative guidance to patients in determining their choice about introducing an IoB device into their lives.

Cyber security risks or not, it's clear that IoB devices are here to stay. We will continue to see impacts on the health, cyber, legal, and ethical domains, amongst others, and it's vital that policymakers act now, as Australia's health security, and ultimately Australia's national security, relies upon it.

Rebecca Banagala is an ANU Masters of National Security Policy student and works in project delivery and implementation for an Australian Government department.

THE IMPORTANCE OF CLIMATE DIPLOMACY FOR AUSTRALIA

Tutti Copping,
University of Technology Sydney

The Australian Government's recent refusal to commit to a net zero emission reduction target following the release of the harrowing Intergovernmental Panel on Climate Change (IPCC) report is another 'F' on its climate change report card. This lack of action comes shortly after New South Wales experienced the worst fire season in recorded history , and the Great Barrier Reef suffered its third iteration of coral bleaching. The latter saw 60 per cent of coral in the reef affected, and serves as a pertinent reminder of the environmental impact climate change is having in Australia.

Climate change policy is often viewed through this environmental lens. But Australia's lack of climate change policy is also affecting its diplomatic relations. When the rest of the world is pushing towards net zero emissions, where does that leave a country like Australia?

Australia's lack of substantive action on climate change is undermining one of its most prominent and necessary diplomatic relationships. The Pacific Islands have become the 'poster child' for the environmental impacts of climate change, with loss of statehood, culture, and the threat of displacement being real eventualities for the region. The effects are already visible, with 80 per cent of all global climate-related migration between 2008 and 2018 occurring in the Pacific region. These consequences are more severe in countries such as Tuvalu, Kiribati, and the Marshall Islands, where a rise in sea levels has caused substantial damage to agricultural lands and drinking water. While in Australia climate change is mainly regarded as political discourse, in the Pacific Islands it is a legitimate existential threat.

With this in mind, it comes as no surprise that the Pacific Islands continue to flag climate change as the biggest threat to their national security. This stands in stark contrast to Australia's policy priorities. In the 2020 budget for example, analysis shows that the Australian Government allocated a mere 16 cents out of every $100 spent towards addressing the climate crisis. This is in contrast to a staggering $10.3 billion given in fossil fuel subsidies in the 2020-21 financial year. These figures illustrate the Australian Government's lack of action on climate change, which has been confirmed by the fact that Australia's emissions have increased by eight per cent in the period between 2005 to 2019. The vast difference in the prioritisation of climate change mitigation between Australia and the Pacific nations is profoundly affecting this diplomatic relationship.

This friction is problematic for Australia, as it is in its own national interest to ensure that the Pacific region remains a stable and prosperous zone. Australia and the Pacific Islands have a long history that has been forged over years of engagement, mutual support, and assistance. Over the past few decades, Australia has worked to help achieve stability in the area, which in turn has promoted stability in Australia. Given Australia's isolation, it is strategically beneficial to maintain a good relationship with these neighbouring countries. Economically, Australia benefits immensely from the established relationship with countries in the Pacific and is actively working to enhance these ties. One only needs to watch the cruise ships leaving Circular Quay for the Pacific Islands to understand the mutual benefits to the tourism industry.

Looking further inland, Australia's agricultural sector is heavily reliant on labour migration schemes established with the Pacific Islands. Reports have found that these schemes aid in combatting the labour shortages in the agricultural sector and also increase productivity levels compared to traditional seasonal labour schemes. These programs are estimated to grow to five times their current size by 2040, reinforcing their economic value and necessity. By alienating Pacific nations through a lack of substantive climate change policy, Australia is putting itself in a precarious position, both in terms of national security and economic prosperity.

Australia's relationship with the Pacific region is getting more difficult to maintain as Australia continues to refuse to act on climate change. At the 2019 Pacific Island Forum (PIF), Australia declined to commit to the climate change objectives set by the Pacific Islands in negotiations. In fact, Australia refused to include any reference to coal, limiting global

warming beyond 1.5 degrees Celsius, or a commitment to net zero emissions by 2050. This lack of support was cemented whenNew Zealand, another key actor in the Pacific, announced its commitment to a net zero emissions target for 2050 in an act of support for the Pacific. Australia's refusal to stand in solidarity with the Pacific Island region demonstrates a cruel indifference to the consequences of climate change on its neighbours.

As these tensions simmer, the Pacific Island nations are turning to other countries for support and partnership, such as China. China has become the second largest aid donor in the region after Australia , and unlike Australia, has committed to net zero emissions by 2060. Other countries, including the United States, New Zealand, and the United Kingdom are following suit, using climate change policy to leverage diplomatic ties in the region. Various Pacific 'resets', 'uplifts', and pledges have been made by countries, in a hope to build on their influence and relations in the Pacific. This international movement shows that action on climate change is the key to establishing and maintaining relations in the Pacific region. Given the disastrous consequences that the Pacific is facing because of climate change, it is evident that the region will cooperate and engage with countries that work with them, rather than those that seek to impose their own interests.

What we see in the deteriorating relationship between Australia and the Pacific Island nations is a case study for what will happen on a larger international scale if Australia continues to neglect to address climate change. As more countries commit to emission reduction targets and move to reduce their reliance on fossil fuels, Australia will be left isolated and distanced from the rest of the world. Australia has already come under intense international scrutiny for failing to implement substantive climate change-related goals. In fact, ambassadors from the United Kingdom and United States met with the Australian Government several times this year to encourage Australia to commit to stronger action on climate change. With COP27 coming up in late 2021, it is imperative that Australia can bring something to the international table to show its commitment towards combatting climate change. Failing to do so has the potential to jeopardise Australia's reputation and relationships on an international level.

It is evident that the key to resolving and dissolving these tensions in the Pacific and on a broader international scale is for Australia to implement a powerful climate change policy. By doing so, Australia not only alleviates the potential harm and environmental damage that will result from climate change, but it will also maintain and improve the diplomatic relationships with its closest neighbours. It should be noted that a common criticism of Australia's policies and programs involving the Pacific Islands is that they are often created without the consultation of the Pacific Island region. When Australia considers implementing a policy on climate change, it should consult with its Pacific Island neighbours to ensure that its policies work to a timeline that assists in achieving their goals. This will both strengthen the relationship and ensure any policy is robust.

For Australia to maintain its relationship with the Pacific Islands, the first step is to implement a substantive and comprehensive climate change policy. Addressing climate change is inevitable, but the longer Australia stalls, the more it risks.

Tutti Copping is a penultimate year Bachelor of Communications (Social and Political Sciences) and Bachelor of Laws student at the University of Technology Sydney.

THE CRISES BEFORE CRISES: MANAGING TENSIONS IN PREPAREDNESS

David Beaumont,
Australian Army Research Centre

In a 2020 statement depicting the confluence of existential national security issues facing Australia, the Chief of the Australian Army, Lieutenant General Rick Burr, impelled the Australian Army to 'adapt for the future'.[1] He has not been the only Australian public official in the last two years to have directed his organisation to dramatically change its approach to prepare for a future of converging crises and requirements. Soon after the preceding version of Accelerated Warfare had been released, Australia endured the 'Black Summer' of 2019-2020 that saw a 'call-out' of the Reserves, and was about to face the COVID-19 pandemic — events that saw the Army committed to a range of crisis responses.[2] Furthermore, a new strategic policy statement was about to be issued preparing the ADF for a difficult and dangerous strategic environment, with strategic competition at levels few had seen since the twentieth century Cold War. It was a time that emphasised how important preparedness planning was, and why further planning was necessary to face a range of potentialities.[3]

The stark reality of crisis responses, whether they be military or not, is that organisations rarely prepare for events as best as they might. This, in fact, is something public policy officials should expect given how complex and complicated preparedness planning really is. This article will describe tensions that often effect preparedness planning and crises responses. It will also provide a few military experiences and ideas that are instructive to public policy officials or response organisations that are considering their own preparedness requirements. Though barely scratching the surface of the topic, the article highlights that preparedness is much more than identifying potentialities and prescribing solutions. Successful responses require much more than that.

Firstly, what is preparedness? This is a deceptively difficult question to answer, and it really can't be answered without context. Dr. Thomas Galvin, writing for the US Army War College, suggests that this question should be replaced by two. First, 'are capabilities on hand prepared for X?' which is a question of readiness. Second, 'are the right capabilities on hand for X?', a question of having the right organisations and methods of coordination.[4] So Galvin follows with 'preparedness' as 'the actions taken to plan, organise, equip, train and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from threats to national security interests.' This in of itself raises even more problems for policy makers. This is not only because preparedness is a 'complex system composed of numerous variables', but that variables can conflict and damage on another especially when choices — and in particular funding choices — are made.[5] To be adequately prepared requires choices to be made amid a tension between making forces 'ready for what' rather than 'ready for when'.[6] Sadly, for frustrated preparedness planners, it is almost always impossible to balance both in public policy making but also in practice.

The idea of being 'ready for when' speaks to the reinvigorated concept of 'national resilience'. Resilience has been described in Government policy making for over a decade, especially in the context of Australian responses to natural disasters.[7] But it became a topic du jour in the wake of the 2019-2020 bushfire disasters, with its relevance increasing with the continuation of the COVID-19 pandemic. The Australian Defence Force somewhat captures this concept in the notion of 'sustainability' which entails the capability and capacity of a military force to remain in operation.[8] But there's more to resilience than simply supporting crises responses over a period of time. Resilience is the ability of organisations, even society, to restore normality after a strategic shock or crises. It is a recognition that we will be unable to accurately predict the future, and that the capacity to respond to crises is more important to than identifying what it is that organisations and society are preparing themselves for.

The 1999 deployment of Australian peacekeeping forces under INTERFET has been cited by historians as an Australian example of poor military preparedness, despite years of preparations for operations that were made. In observing the operation and a range of other small peacekeeping missions, historian Bob Breen blamed 'ad hoc, inefficient

and complicated arrangements', that created the conditions such that 'the ADF was neither as proficient as it thought it was, nor competent as it should have been'.9 But the reason that several thousand Australian soldiers lacked suitable equipment or deployed in an uncoordinated mass had as much to do with Defence being unable to manage reform and resourcing than it did with its competency. The operation occurred after a decade of structural and business reform, amid the replacement of military hardware, after a recession in which Defence resources were cut, and with internal conflict over how to implement strategic policy. This mess of activity saw tensions in preparedness manifest in an inefficient crisis response, with acute Government attention and auditor investigations afterwards.10 The operation was a strategic success, but the crisis response was far from elegant!

Given the sheer multitude of choices involved in preparedness planning it is understandable why crises responders virtually always appear on the backfoot at the beginning of any disaster — it is often beyond the capacity of even the most well-resourced national agency to precisely predict what future requirements may be and prepare accordingly. Policy makers and creators responsible for preparing for crises responses must identify threats, think about what capabilities are needed to offset or respond to threats, time the availability of the capabilities to maximise their effect, determine how long these capabilities must operate for and how resilient they are to surprise or shock they are!11 But it remains important to engage with preparedness issues and think about crisis scenarios, for the act of planning tests organisational systems and capabilities, as it is to consider practices and identify risks that ultimately contribute to the resilience of the systems and methods of coordinating national security agencies that must respond effectively in a time of crisis. As the adage goes, and is paraphrased here, the act of planning could very well be more important than the plans themselves. This may have factored in the outcome of the military operation described above.

The ADF thinks about preparedness issues, and potential threats and activities, every day and is fuelled by lessons from the past. It doesn't always get it right for reasons described above, but lessons from military experiences in creating effective preparedness systems are relevant to the national security enterprise. These lessons present consistent themes and issues for planners to consider. Firstly, policy and strategic guidance is essential to assist in the prioritisation of resources to preparedness outcomes. Secondly, response organisations must be structured to plan, and adequately supervise, any response that is needed. Response organisations must be provided with the right capabilities and resourced relative to the tasks required; this prevents waste and allows precious resources to be directed to other needs. Fourthly, internal planning must emphasise the sharing of knowledge with plans disseminated so all involved know exactly what they should be doing, and a mutual understanding permeates the organisation. Finally, and most importantly, response agencies must be practiced and exercised such that any response to a crisis is reflexive. Although these five themes seem trite and an oversimplification, addressing each of them helps to create systemic resilience and improves crisis responses.

Preparing for crises is one of the most important things that the ADF does — it is one of the most important things that the national security enterprise must do. Since 2019, Australia has endured circumstances that have brought preparedness thinking to the fore and elevated somewhat dormant ideas such as resilience to headline public policy statements. In concluding this short article, and reflecting on lessons from military thinking about preparedness, it is important to recognise that preparedness planning is a process and a practice — no planner should feel comfortable creating arbitrary plans and leaving them on a metaphorical shelf to be used when needed. Planning is an adaptive process, as a practice. Any national security organisation serious about its obligations to the community at large cannot lull in its consideration of the problems of the future and how the organisation will need to respond. It must navigate the tensions resident within the problem of preparedness, and leaders will have to make decisions that are always influenced by assessments of risk and defined by compromise. While these decisions may not always be the correct ones, the effort already taken, will come a long part of the way to assuring resilience and responsiveness when the nation needs it most.

Colonel David Beaumont is the Director of the Australian Army Research Centre which provides research support and advice to the Australian Army. He is a military logistician by background and has served in major crises responses including stabilisation missions and disaster relief. David is currently undertaking PhD research within the Strategic and Defence Studies Centre, Australian National University, analysing the logistics factors leading to preparedness problems prior to INTERFET in 1999. He also writes at www.logisticsinwar.com, and has authored numerous papers and articles for the Australian Army.

Australian Crisis
Simulation Summit