AUSTRALIA'S AI STRATEGY

EMBOLDENING THE POTENTIAL FOR AI COLLABORATION
THROUGH THE TRILATERAL SECURITY DIALOGUE

Australia's Artificial Intelligence Strategy Emboldening the potential for AI collaboration through the Trilateral Security Dialogue

Trilateral Security Dialogue
Paper Series No. 2

Melbourne

Authors

Aiden Warren
Charles T. Hunt
Matthew Warren
Adam Bartley
Mark Manantan

ACKNOWLEDGEMENTS

EXECUTIVE SUMMARY

The Australian federal government has grown increasingly active in the Artificial Intelligence (AI) space over the past five years with key strategy documents relating to the use and development of AI, data policy, digital economy, and defence guiding much of the nation's direction in this pivotal area. While much is currently made of Australia's Artificial Intelligence Research and Development capabilities, the foundations to a compounded investment in AI face critical challenges in terms of investment, talent shortages, intergovernmental adoption, and security concerns across the information and cyber, maritime, air, space, and land domains.

In the context of defence, Australia's engagement across AUKUS (Australia, United Kingdom, United States), the Quadrilateral Security Dialogue (Quad), and the Trilateral Security Dialogue (TSD) indicates a more robust response to AI and, more generally, emerging technologies. Despite these initiatives, however, investment in defence and global defence partnerships have come at the cost of investment potential within strategic sectors of the Australian domestic environment, including higher education. In the defence, diplomacy, economic, and military domains Australia is recognised as a middle power, capable of steering regional governance platforms and amplifying global institutional frameworks. However, it has at times adopted a cautious mindset in the AI field, producing fears that without a cultural change in the areas of experimentation, knowledge discovery, and creation, Australia will remain a pedestrian "taker of AI" only.

In tackling these concerns, the second Trilateral AI Experts Group dialogue was held in Melbourne, Australia, to examine these gaps in an Australian context. As part of a broader Department of Defence Strategic Policy Grants Program (SPGP) project that examines strategies for enhancing Australia's AI capability development and defence cooperation with Japan and the United States under the Trilateral Security Dialogue (TSD) framework, the synthesis below offers a brief analysis of the key challenges across the domains of AI security, development, and interoperability. In tracking insights across Australia's AI landscape, the researchers include recommendations at the document's conclusion.

INTRODUCTION

This report examines the AI development and regulation policy space in Australia and assesses congruity of purpose across partner and national strategies, data development, defence alignment, and interoperability. Broken into three sections, the first investigates Australia's non-defence-related policies and decisions made in the AI space and evaluates the extent to which strategy frameworks have been addressed either via government implementation or policy. This section seeks to examine AI readiness in government as defined by the aspirational goals set out in the various public facing strategy documents. The second section widens the aperture on Australia's defence strategy concerning the development of AI and the areas and challenges for collaboration with TSD partners. Here, the report responds to the common themes of AI security, interoperability,

istockphoto / Bionics Exoskeleton Prototype

> HOWEVER, IT HAS AT TIMES ADOPTED A CAUTIOUS MINDSET IN THE AI FIELD, PRODUCING FEARS THAT WITHOUT A CULTURAL CHANGE IN THE AREAS OF EXPERIMENTATION, KNOWLEDGE DISCOVERY, AND CREATION, AUSTRALIA WILL REMAIN A PEDESTRIAN "TAKE OF AI" ONLY.

development, and ethical considerations. The final section presents recommendations for addressing Australia's AI shortcomings.

AI SECURITY: AUSTRALIA'S AI STRATEGY AND POLICY LANDSCAPE

Australia's AI Action Plan (AI Action Plan or "the plan") was established in 2019 by the Morrison government and attempted to provide much needed clarity on the government's vision for AI and to the importance that such critical technological developments would play in Australia's future. The plan outlines that an enhanced understanding about the utility of AI and its broad application across society is required.[1] In developing a pathway for AI implementation and development, the plan leverages existing strategy foci exemplified in state governments across Queensland, New South Wales, Victoria, and South Australia, and CSIRO's Artificial Intelligence Roadmap.[2] More generally, the strategic levers of AI growth are synthesised across five themes: AI commercial innovation; talent acquisition and growth; AI health, disaster, and national interest innovation; and, global AI leadership. The plan is complimented by further strategy documents in the Digital and Data Government Strategy (Government Draft for Consultation), which has contributed up to AUD$1 billion via the Job Trainer Fund and Digital Skills Organisation in 2022, while a more comprehensive outline of the government's technology agenda is reflected in the Digital Economy Strategy 2030.[3]

The Australian government has also invested in several multilateral initiatives that join in advancing principles and standards on ethics across governance platforms. These include the Global Partnership on AI and the Organisation for Economic Cooperation and Development (OECD) Council Recommendations on AI. Australia is also a party to the United Nations (UN) Framework for Responsible State Behaviour in Cyberspace; a member of the UN Group of Governmental Experts (GGE) process underway within the Convention on Certain Conventional Weapons (CCW); and has initiated the ASEAN-Australia Digital Trade Standards Initiative. Bilaterally, further endeavours include the Australia-US Frontier Tech Dialogue, the Australia-US Digital

Trade Agreement, the Australia-India Cyber and Critical Tech Partnership, the Australia-Singapore Digital Economy Agreement, and the Australia-UK FinTech Bridge.

Beginning in 2019, these measures produced an ostensibly active AI and cyber program for the Australian government. Spending themes outlined in the AI Action Plan were set to roll out across a four-year program beginning from fiscal year 2021-2022. Across three key risks identified by The National Science and Technology Council's joint report, Rapid Response Report: Generative AI, Australia has done remarkably well in transitioning workers to other tasks and roles as facilitated by AI, managing AI responsibly, and enabling equal access to generative AI across businesses and individuals.[4] These include initiatives across government and research bodies such as CSIRO, and encompass the Responsible AI Network for improving industry governance capabilities, the AI Ethics Framework, and Department of Industry, Science and Resource's Safe and Responsible AI policy.

Over a year into the Albanese era, however, AI development and spending has slowed appreciably.[5] In looking for alignment across the new agenda, the Labor government has reduced the AI budget, jettisoning the $44 million plan to fund four strategic AI and Digital Capability Centres. These were to provide a "front door" for AI development among small to medium enterprises (SME). While the Albanese government also sought to drop the

Advanced Strategic Research Agency announced in 2022, it has promised to invest $3.4 billion over the next decade for an Advanced Strategic Capabilities Accelerator (ASCA), which will amount to a spending increase of $591 million above current planned spending on defence innovation.[6] ASCA will prioritise a range of emerging technologies including hypersonics, quantum computing, information warfare, and Long Range Precision Fire (LRPF) Missiles. While AI is not an explicit designation under ASCA, its programs will address AI-enabled shortcomings and aid collaboration across Defence and industry.[7] It is worth noting that while many stakeholders interviewed for this project emphasised Australia's ability to develop above its limited capabilities in the AI space, they all agreed that this capacity was diminishing and Australia was likely to drop in global AI development terms, by considerable margins, as government investment, regulation, and interest lags.

AI DEVELOPMENT: POLICY CHALLENGES

The abovementioned changes brought about by the current government have occurred in the context of a rollout of the AI Action Plan that was already

CPL Nunu Campos / Australian Army

slow under the previous Morrison government. $33.7 million allocated for the national challenges program, for instance, was never delivered. And over the first year, only one third of the annual spending plan for AI was allocated across the CSIRO-led National AI Centre and the Next Generation AI Graduates Program.[8] At a more granular level, the plan sought to shore up a world class AI talent environment with the commitment of "more than $200 million" in Australian Research Council (ARC) grants and fellowships for projects that address AI. However, the ARC and associated research endowment, which covers all disciplines of university and research enquiry, has been consistently trending downwards, as funds are redirected elsewhere in the national budget.[9] In other words, the AI Action Plan in its original form claimed support for AI in research and development that already existed, and whose researchers face increasing roadblocks to accessing funds due to the highly competitive and restrictive ARC applications and funding opportunities.

The Albanese government, meanwhile, has not sought to update the AI Action Plan beyond encouragement for new regulation, for instance, releasing a Safe and Responsible AI in Australia Discussion Paper and The National Science and Technology Council's Rapid Response Report: Generative AI. While developing "appropriate safeguards to ensure the safe and responsible use of AI"[10] has become a focus for the government, fears that an even more conservative approach to AI is being pursued have arisen. The Royal Commission into the Robodebt scandal, an automated debt assessment and recovery program housed under Centrelink's Online Compliance Intervention Program, underscores the challenges AI will likely continue to face in the current government, both as a function of the Australian Public Service (APS) and as a culture defining example. While Robodebt was not an AI-enabled platform, the algorithm employed did automate the use of data-matching to issue debt notices to Centrelink welfare recipients.[11] The government at the time failed to create oversight tools and other safeguards to counterbalance the flaws in the algorithm, leading to a system that overcharged welfare repayments by a 27 percent margin.[12]

The Robodebt example illustrates the drastic need to rebuild trust with the Australian public around automated services that will inevitably include AI in the future. The government has emphasised the need

ONE REPORT RELEASED EARLIER THIS YEAR REVEALS THAT AUSTRALIAN BUSINESSES ARE INCREASINGLY HAVING TO TROUBLESHOOT AI INTEGRATION SYSTEMS IN THEIR COMMERCIAL NETWORKS ACROSS MULTIPLE AI TECHNOLOGY AND SERVICE PROVIDERS DUE TO TALENT SHORTAGES IN AI STRATEGY, DATA ANALYSTS, AND AI OPERATIONS.

for principled AI governance across government and industries sectors, but it has done so while also delaying further action on the development of a more comprehensive AI strategy and plans for developing reliable AI systems across government. The Digital Economy Strategy 2030, for instance, provides little clarification about the integration of digital strategy and AI, or how new data forms can be integrated across government and industry. This is likely to have serious implications for building AI culture in the APS, which is already viewed as falling short of skills and initiative.[13]

Insights from the workshop in Melbourne underscore the challenges this culture and funding lethargy will have on developing an AI-ready workforce and ecosystem across the APS, private sector opportunities for AI development, and education and training. Indeed, more recent attention to brain drain in AI and data research professionals demonstrates that the talent retention and recruitment problem is much more of a national risk.[14] CSIRO's Australia's AI Ecosystem Momentum Report released earlier this year reveals that Australian businesses are increasingly having to troubleshoot AI integration systems in their commercial networks across multiple AI technology and service providers due to talent shortages in AI strategy, data analysts, and AI operations. Meanwhile, corporations and particularly SMEs are increasingly having trouble finding AI providers who offer end-to-end support.[15] In other areas, this has led to ease of access issues with implications for data and cyber security because corporate members, to create workarounds from cloud computing issues often housed offshore, for instance, have opted for secondary physical data storage locations, which are more susceptible to hacking.

The national shortage of AI professionals is compounded by the intense global competition for

AI services, which has priced the salaries for such professionals out of reach for many small to medium enterprises in Australia. In the APS, interviews and workshops with stakeholders reveal a broader contest for talent, where departments are forced to borrow data scientists, rather than hire them, imposing further costs on tax payers. In some cases, consulting companies have poached entire teams from government AI work groups, who have then gone on to consult on government projects with diminished support systems.[16] In October 2022, Minister for Industry and Science Ed Husic warned that delays in supporting the AI Action Plan would ensure Australia's AI talent challenges would worsen.[17] However, except for continued funding under the Plans' funding for STEM graduates, there appears to be limited plans to develop talent acquisition further across the APS or address emerging cultural norms that keep AI applications at arm's length.

DEVELOPING AI SECURITY

These shortcomings raised concerns among workshop participants for data sovereignty. Funding limitations that push the APS or companies to rely on third parties for AI and cyber-related services increase the reliance of government on software companies that may not be located in Australia. Data breaches, software malfunctions, infrastructure breakdown, inaccurate models, cyber intrusions, and other challenges that may require fast-action responses with delicate data pools may not be addressed efficiently or may require offshore third parties to first meet regulatory requirements before action is taken. These concerns, highlighted by workshop participants, speak to a skilled labour challenge, but also a cultural challenge that may make AI adoption within government, and with the use of important but delicate data pools, more difficult. A strong fear is that the culture around adopting technology, and not developing it (former Prime Minister Scott Morrison's remarks that Australia would become the best "technology adopters" was widely condemned), has become embedded within government.

Additionally, current domestic-facing Australian strategy documents omit the critical importance of international partnerships that a low budget approach to AI will inevitably necessitate. There are some isolated examples of international collaboration, but these fall short of offering the whole of government approach advocated. For instance, the National

Artificial Intelligence Centre, currently hosted in Data61 at CSIRO, invited applications in 2022 for the National Science Foundation (US) AI Research Collaboration Program but restricted funding to a maximum of AUD$800,000 over three years. There is no indication the program is ongoing.[18] In other areas, individual, but ongoing, ARC Discovery, Linkage, and Fellowship funding may contain an international collaboration component, but these are less geared toward national strategic aims for AI and more for general research which may contain AI-related components.

Successful examples of America's international partnerships highlight the need for more cross-national funding and for Australia to move beyond remaining an "AI taker" attached to a Hub and Spokes system in the United States. The U.S. Office of Naval Research Global's (ONRG) research bases in Australia and Japan have had considerable success in building "soft standards" – habits of standardisation in practice and design – in the absence of legal and/or codified norms. Standards were considered by workshop participants to be one of the more challenging components for AI collaboration, particularly in the case of Australia-Japan collaboration where more incongruity exists in basic definitions, operational behaviour, and defence employment. Additionally, the ONRG's offices have been useful in integrating research complementarities and exposing US researchers to further AI capabilities that might otherwise have remained latent in an isolated national setting. Australia's limited international partnerships, by contrast, stands as an inhibiting factor that may stymie greater innovation and thus economic development across AI-enabled platforms. Studies by researchers at Waseda University in Tokyo on

LTCOL David Hankin / Australian Army

international cooperation in innovative technologies and research have found that "geographically diversified knowledge networks" tend to be more innovative and productive than domestic networks. Without leadership on the issue, Australia's AI capabilities may begin to fall rapidly further behind.[19]

Meanwhile, an attempt to redraw norms on rapid prototyping in government and defence has produced considerable excitement among US researchers, with strategic communities and leadership bringing weight to bear on ideas for AI integration.[20] While such communities in Australia do exist, particularly in the Defence Science Institute and the Defence Science and Technology Group, the depth of engagement has been limited by an overreliance on collaboration with culturally like-minded partners (US and UK). Without further funding and concerted partnership building efforts, TSD partnership is likely to remain largely diplomatic and high on symbolism.

Across all three TSD nations, R&D spending on AI overwhelmingly takes place in the private sector, with cutting edge-fields also occurring outside of government labs and traditional defence companies.[21] In this light, research examining differences between aspiration and reality in national AI strategies, reveals that while countries like the United States and Japan have developed a technology-prepared workforce, Australia has fallen into the category of unrealised aspirational potential.[22] These points illustrate that in the absence of new oxygen to a more comprehensive and well-funded AI development agenda, the search for a world class innovative AI society that can reach the top end of economic productivity projections (as outlined in Rapid Response Report: Generative AI) may be beyond reach.

AI INTEROPERABILITY: POLICY IMPLICATIONS AND CHALLENGES

Interoperability is the ability for organisationally and culturally differentiated units or systems to operate effectively to produce an efficient and congruent outcome of purpose.[23] Forces or systems adopt interoperability to bring force multiplier effects and innovation to challenges seen as beyond the capabilities of individualised or isolated units. For AI, interoperability across national governments or militaries calls attention to AI-enabled outputs that may exist in one nation for employment

Shutterstock / swarm drones

across separate national defence systems for force integration and deterrence. Currently, there is great interest and discussion on how states like Australia may contribute to AI interoperability across force partnership agreements like AUKUS, the Quad, and the TSD.[24]

In Australia, discussion in this space has occurred primarily around the new aspirations for national defence security in the 2020 Defence Strategic Update (DSU) and the 2023 Defence Strategic Review (DSR). While the DSU significantly shifted national attention toward new and emerging technology areas, including cyber, as domains for special attention and new spending, the DSR reinforced this attention with a focus on AUKUS pillars I and II. This evolution in defence strategy documents also occurred within the Royal Australian Navy and more broadly across the departments in defence. The Plan Mercator Strategy 2036, for instance, for the first time highlighted the importance of AI-enabled platforms as a more detailed feature of force planning.[25] The 2020 Robotics, Autonomous Systems and Artificial Intelligence (RAS-AI) 2040 strategy, and its Army counterpart, RAS v2.0, give more detail and strategic guidance across broader Defence in AI. Both documents have contributed to groundbreaking exercises using automated and AI systems. Autonomous Warrior 2022, for instance,

STANDARDS WERE CONSIDERED BY WORKSHOP PARTICIPANTS TO BE ONE OF THE MORE CHALLENGING COMPONENTS FOR AI COLLABORATION, PARTICULARLY IN THE CASE OF AUSTRALIA-JAPAN COLLABORATION WHERE MORE INCONGRUITY EXISTS IN BASIC

included more than 300 personnel from the US, UK, New Zealand, and Australia with key industry partners across a range of AI-enabled systems in the maritime domain.[26] The more recent AUKUS AI and autonomy trial in Belfast UK, included "live retraining of models in flight and the interchange of AI models between AUKUS nations" – a world first in leading technology integration and interoperability.[27] As one participant remarked, these AI trials have shown that the technical challenges for AI and autonomy interoperability are able to be broken down with the right policy mechanism to enable them.

Across AUKUS pillar II and the Quad Critical and Emerging Technology Working Group (CETWG), an AI transformation in critical technology exchange and collaboration is currently taking place. One account from the Center for Strategic and International Studies (CSIS) suggests that Pillar II may in fact be more substantive than Pillar I, given the transformational characteristics of its focus on AI, quantum computing, semiconductors, biotechnologies, and synthetics. The Quad CETWG has been comparatively less visible and focused predominantly in the diplomatic domain on principles of technology standards, telecommunications, monitoring trends in critical technologies, and dialogue on technology supply chains.[28] There is some potential for AI collaboration across Indo-Pacific Partnership for Maritime Domain Awareness (MDA), an initiative that integrates commercially available satellite image data across the Pacific islands, Southeast Asia, and the Indian Ocean region to improve information sharing.[29] The opportunity for further AI-enhanced activities, particularly with the use of commercially or publicly available data, the MDA illustrates, is much greater than currently being pursued. As some military commentators have remarked, "The scope of the working group is, so far, fairly modest."[30] Part of this challenge is demonstrated by the bilateral approach to collaboration. For instance, Japan and India signed a digital partnership agreement in 2018 to link Japanese investors with Indian startups. In 2021, the United States and India launched an AI intelligence initiative to develop further bilateral R&D collaboration. Meanwhile, Australia, Japan, and India all have strong AI network collaboration partnerships with the US, but between each other these networks are sparse.[31] The Quad Investors Network will likely build on collaboration, but the results may be selective, and in India's case, limited by strict foreign investment review processes designed to insulate critical technology industries.

Despite these developments, however, the fragmented nature of collaboration has stymied more holistic efforts with implications for interoperability. Even with these changes, "fundamental shifts in strategy and tactics from the AUKUS partners," and particularly for Australia in having to prove that it has the "capability and capacity [to] pursue such a complex multifaceted endeavour" will consume much of Australia's collaborative capacity.[32] In the Quad, some have noted, opportunities to facilitate defence collaboration in the emerging tech fields have not been sufficiently networked or standardised.[33] While standards between Australia, the US, and the UK are quite close, with language, legal, and political similarities that breakdown barriers, this is less likely the case with Japan, and even more so India, with implications at both the operational and strategic levels of AI partnership.

Additional collaboration across borders is being pursued via the Five Eyes group (Australia, Canada, New Zealand, UK and the US) under the Technical Cooperation Program (TCP). The TCP has depth of culture, cohesion, and confidence built into the grouping as a result of its long-term partnership and language complementarity. In 2017, the US Congress added Australia and the UK to the legal framework of National Technology and Industrial Base (NTIB), which has led to new opportunities for joint R&D and technology transfer between the three nations, as demonstrated more recently in AUKUS. This treaty allows Australia and the UK to skip much of the overhead caused by regulations and trade back and forth without licencing.[34] The Five Eyes members also have strong standardised operating practices and technical specifications that allow for smoother military transference and training, and, in the AI space, greater room for data sharing and AI development.[35]

The TSD by comparison is less developed for critical technologies and AI collaboration than its counterparts. Japan is not party to the NTIB, and broader knowledge about Japanese export restrictions has added complexities for countries like Australia when dual-use items for defence or commercial use are included. However, recent changes with Japan's National Security Strategy have produced significant policy shifts across spending and collaboration themes, which have included reform to export controls

and reducing bureaucratic red tape. More recent cooperative defence joint efforts between Japan, the UK, and Italy in the Global Combat Air Program to produce sixth generation jets demonstrates that it is actively seeking stronger international collaboration with like-minded partners. According to some, Japan sees the TSD relationship as an ideal forum for collaboration. With historic changes to defence spending, particularly around emerging technologies and AI, Japanese defence companies, including burgeoning smaller ones, are seeking international partnerships for growth and development.[36]

STANDARDS AND DATA

These international partnerships illustrate that codifying standards will be key for further interoperability of systems, not just across defence applications, but also in the private sector and among the APS. Building in "Pathfinder" projects will help to deconflict existing agreements under the TSD, for instance, across export control regimes. There is momentum in the United States to reform the NTIB, which may include adding Japan to the list, substantially enabling TSD AI collaboration while developing habits of cooperation for AI interoperability.[37] Another initiative emerging is the potential for Privacy Enhancing Technologies (PETs) to increase shared access to public data sets for AI training and testing. This has been recognised at the

highest levels of American policy making, with US National Security Adviser Jake Sullivan making the case that PETs offer a promising area "to overcome data privacy challenges while still delivering the value of big data." Further discussion around creating a shared interface through CloudBank seeks to help incubate "an international network of research universities collaborating on these technologies," writes Imbrie and others, which could revolve around providing cloud computing credits to researchers without access to large and diverse data sources.[38] This would require governments to approach agreements with a focus on safe harbour laws and data consortia agreements that allow for controlled experimentation, while preserving privacy.

In Australia, the Defence Data Strategy 2021-2023 deliberately tackles these challenges through the creation of its enterprise-wide data division with a focus on managing data as a new national asset. The document is rudimentary and a little tardy, but nevertheless an important beginning for the realisation of AI collaboration across borders. Importantly, it underscores many of the challenges addressed above that require immediate redress to move the Department of Defence into a technologically capable fourth generation force. These include low departmental data literacy, an inability to search across agencies for data assets, data workforce imbalances across defence public service, defence force and industry personnel, and not being

aligned with Australian Government, Five Eyes, and best practice standards, which currently make lifting data maturity more difficult.[39] While the document does not mention the prospect of employing PETs across systems to build in data training, the focus on an agile data program will necessarily incorporate new and novel approaches to AI development.

ETHICS

The Artificial Intelligence Ethics Framework has ensured Australia is a world leader in ethical principles and on discussions about reliable AI. Further continuity with like-minded documents in the US and the EU underscore a congruity of purpose that is likely to ease cross-border collaboration. However, the fast-paced development of AI demonstrates the necessity for ongoing development. For instance, Chat GTP has become increasingly essential for researchers and SMEs, and while safety features have been built in to prohibit criminal or violent activity, these have shown to be easily bypassed.[40] Other examples such as the Robodebt scandal outline how AI can be easily misunderstood without human oversight. Another takeaway from this example is the ease with which AI can be manipulated by malicious actors. This underscores the need for robust standards, as aforementioned.

Questions also raised in the workshops drew attention to the costs of not employing public AI data sets for public interest due to privacy concerns. Google's AI company Deepmind attracted significant public animosity when it was employed to trawl through 740,000 records of the UK national healthcare system. The outcome, however, was an algorithm that helped to diagnose critical kidney failure much quicker than had normally been the case. Outlining the clear public benefits with transparent initiatives is likely to offer partial mitigation of a broader public aversion to AI-enabled tools that use public and private data. Finally, sandbox experimentation – to help build understanding and exploration in the explainability problem of AI – will help militate against the concerns of, on the one hand, the potential for exploitative uses of AI and, on the other, the quashing of innovation through over-regulation.

RECOMMENDATIONS

1. The Albanese government should initiate an AI research security dialogue.

The Albanese government should facilitate a dialogue that would allow government departments to create a robust and strategic AI research corridor among TSD partners. For broader understanding, interaction, and time saving, this dialogue should include key members of applicable commissions and committees in all three states. A further component would be the establishment of new networks to begin building an ecosystem of AI innovation. With each state driving national innovation towards such systems at varying levels, they are also currently doing so in isolation, and with separate ambitions in mind. Addressing and unifying bureaucratic and conceptual gaps could foster this development and streamline the processes of exchange.

2. The Albanese government should advocate for a TSD framework of cooperation across guiding principles and standards.

A principles framework for TSD partnership would foster: (a) a very clear understanding of Australia's AI values and vision for collaboration; (b) commitment by Japan and the United States to agree to a timeline of engagement. This would lead to an exchange and understanding of interpretations of principles; a joint agreement on ethical uses, applications, and employment of AI; and, the basis for a diplomatic approach to standards setting in AI internationally; (c) develop strong trilateral, cross-sector AI partnership, encompassing common standards that will help to build trust in AI exchange, development, and security within and across borders.

3. The Albanese government should advocate for TSD member states to undertake more military exercises with specific AI-targeted training and interoperability.

TSD military cultures vary greatly, and joint exercises help to identify and overcome errors and miscommunications in real-time scenarios. Regular (e.g. bi-annual) rotationally hosted joint exercises promise to improve the deployment of AI enabled technologies and equipment, and provide an avenue to encourage requisite risk-acceptance activities among service personnel and militaries as a whole.

4. Update the AI Action Plan to reflect new realities of spending themes in Defence and across government.

The Albanese government could improve upon current AI strategy documents by providing more detail on execution and lines of responsibility, especially in bridging whole of government efforts. While the current strategic framework provides some detail on how success can be judged, the omission of more specific performance metrics is discouraging, particularly with respect to coordination between government departments and between federal and state authorities. This will help Australia's AI strategy move from the aspirational to successful implementation. In this respect, research reveals that substantial investment in public-private partnerships in AI development is required.[41]

5. Strengthen data and AI skills of APS and build relationships across government for strong collaboration.

There is a concern that the focus of AI development in the Defence sectors may overbearingly crowed out resources and expertise in the APS leading to a differentiated capability between Defence and other Government sectors. This is likely to have a net negative impact in broader collaborative efforts as APS struggles to keep up with leading Defence innovations and agreements that demand more from a limited skilled workforce. To operate 'at scale,' broad data literacy, lines of accountability, and shared responsibilities for maximising outputs will require relationships across government for strong

collaboration and increasingly a national APS data and AI skilled recruitment drive.[42]

6. Authorise a public lead for data development and integration across government.

Both strategy documents underscore the need for data accessibility for ready-to-use AI models and applications. Because data will continue to increasingly dictate the speed of modern warfare, fast and accurate accessibility to data will be crucial to government, defence, and intelligence employment. This recognition permeates strategy documents, and it has become routine for the government to call for a whole of society approach to AI and development. In practice, as interviews with leading Australian thinkers on AI and data reveal, outdated procedures and a large bureaucracy have become burdensome. As data will become a strategic national asset, with force multiplier effects, its integration requires a strategic agenda empowered with leadership and authority. Appointing a public lead for the development and integration of data across government would help in overcoming this inertia and impediments.

7. Develop more regulatory sandboxes to enhance regional collaboration.

Regulatory sandboxes will help move AI projects and collaboration forward by understanding the legal, compliance, ethical, and linguistic hurdles that government and the military must consider. While such sandboxes currently do exist, a more holistic effort that brings together teams from university research institutes, APS and Defence, and industry will further aid understanding, particularly in a transnational context. These sandboxes can exist across technical and legal domains. For instance, researchers and technologists experimenting with applications may be temporarily exempt from regulation that may otherwise be too prohibitive, troublesome, or time consuming. This will help in the early critical phases of experimentation to understand whether applications will have merit. Regulatory sandbox projects can be relatively low-cost while providing government, as well as industry and other researchers, expertise in cross-border research environments.

8. Establish more "pathfinder" programs to accelerate AI development.

Pathfinder programs like the Air Force's Ghost Bat uncrewed aircraft not only demonstrate that Australia has the capability to develop indigenous AI platforms, but that Defence, Government and industry partnership can work coherently in that pursuit. In the US, these programs operate across a broad range of military and commercial arrangements with talent finder initiatives like ONRG. These should be replicated in Australian programs with seed funding directed to specific cross-border collaborations, such as between Australia and the US. Doing so would broaden Australia's innovative capability and branch out from platforms of convenience in AUKUS and Australia-US research arrangements. These programs will also work to deepen the soft-standardisation approaches to AI development that emerge through habits of cooperation.

9. Encourage stronger ethics and debate for off-the-shelf variants of AI.

The rapid emergence and uptake of Chat GTP underscores the utility, and also the vulnerabilities, of off-the-shelf variants of AI. Government programs should be established to begin discussions about these uses and vulnerabilities at the primary and high school levels to build knowledge and capabiltilies from an early stage. Such programs can occur through federal and state government partnerships, and with universities. Additionally, as off-the-shelf AI becomes increasingly mainstream it will be useful for workarounds in troubleshooting other platforms. There is likely to be strong pushback by government and particularly Defence to include such systems within operations. But to ignore their creative use would be costly. As the war in Ukraine has highlighted, innovative defence forces that can adapt and employ heterogeneous systems for multiple operations will be at an advantage over adversaries. Open-source AI and data will be helpful, but this requires a dedicated and ongoing discussion in Australia about how these systems can be safely employed and scaled.

ENDNOTES

1. Australia's Artificial Intelligence Action Plan. Australian Government Department of Industry, Sciences and Resources, 18 June 2022. Accessed via https://www.industry.gov.au/publications/australias-artificial-intelligence-action-plan

2. Insight – Artificial Intelligence to Drive Australia's Economic Growth, Australian Trade and Investment Commission. Accessed 19 August, 2023 via https://www.austrade.gov.au/news/insights/insight-artificial-intelligence-to-drive-australia-s-economic-growth; Artificial Intelligence Strategy, Digital NSW, Government of New South Wales, accessed 19 August, 2023 via https://www.digital.nsw.gov.au/policy/artificial-intelligence/artificial-intelligence-strategy

3. Data and Digital Government Strategy: The Data and Digital Vision for a World-Leading APS to 2030. Australian Government, n.d. Accessed via https://www.dataanddigital.gov.au/; Digital Economy Strategy 2022 Update Released, 30 March 2022. Accessed via https://www.pmc.gov.au/news/digital-economy-strategy-2022-update-released

4. Australia's Generative AI Opportunity. 2023. Mircosoft and Technology Council of Australian, Accessed 4 August, https://news.microsoft.com/wp-content/uploads/prod/sites/66/2023/07/230714-Australias-Gen-AI-Opportunity-Final-report.pdf

5. Aiden Warren, Charles T. Hunt, and Mark Manantan. 2023. Australia's Critical Test for Future Growth: Moving the National AI Strategy from Rhetoric to Reality. Australian Outlook, 20 January. Accessed via https://www.internationalaffairs.org.au/australianoutlook/australias-critical-test-for-future-growth-moving-the-national-ai-strategy-from-rhetoric-to-reality/

6. Hayley Channer and Miah Hammond-Errey. 2023. Australia's Capabilities Accelerator will Need to Break New Ground. The APIS Strategist, 10 July. Accessed Via https://www.aspistrategist.org.au/australias-capabilities-accelerator-will-need-to-break-new-ground/

7. Government Announces Most Significant Reshaping of Defence Innovation in Decades to Boost National Security. 2023. Australian Government Department of Defence. Media Release, 28 April, accessed 4 June https://www.minister.defence.gov.au/media-releases/2023-04-28/government-announces-most-significant-reshaping-defence-innovation-decades-boost-national-security

8. Ibid., See also Joseph Brookes. 2023. Australia's AI Policy, Programs on Ice. 16 March, accessed 18 July, https://www.innovationaus.com/australias-ai-policy-programs-on-ice/

9. Anthony King. 2019. Australian Basic Research Squeezed as R&D to Fall to Lowest Level for Decades. Chemistry World, 16 August. Accessed via https://www.chemistryworld.com/news/australian-basic-research-squeezed-as-randd-to-fall-to-lowest-level-for-decades-/3010856.article; Joseph Brookes. 2023. Research Funding 'Crisis' Overlooked in Budget. Innovation Aus, 11 May. Accessed via https://www.innovationaus.com/research-funding-crisis-overlooked-in-budget/; Innovative Research Universities. 2023. Major Trends in University Research Income and Expenditure. IRU Discussion Paper, March. Accessed via https://iru.edu.au/wp-content/uploads/2023/03/Major-trends-in-university-research-income-and-expenditure.pdf

10. Safe and Responsible AI. 2023. Media Release, Minister for Industry and Science, Australian Government. 1 June. Accessed 3 July, https://www.minister.industry.gov.au/ministers/husic/media-releases/safe-and-responsible-ai

11. Royal Commission into the Robodebt Scheme. 2023. Report Volume One, 7 July, accessed 8 August, https://robodebt.royalcommission.gov.au/publications/report

12. Tapani Rinta-Kahila, Ida Someh, Nicole Gillespie, Marta Indulska & Shirley Gregor (2022) Algorithmic decision-making and system destructiveness: A case of automatic debt recovery, European Journal of Information Systems, 31:3, 313-338

13. Alex Antic and Tania Churchill. 2023. Data and Digital Strategy a Good Start but APS Culture Remains the Stumbling Block. The Mandarin, 22 May. Accessed 12 June, https://www.themandarin.com.au/220833-data-digital-strategy-good-start-but-aps-culture-is-stumbling-block/

14. The Missing Link in Morrison Government's AI Strategy, Financial Review, 13 May, 2021, accessed via https://www.afr.com/chanticleer/the-missing-link-in-morrison-government-s-ai-strategy-20210512-p57rbf

15. Australia's AI Ecosystem Momentum Report, CSIRO National Artificial Intelligence Centre, March 2023, accessed via https://www.csiro.

au/en/work-with-us/industries/technology/National-AI-Centre/AI-Ecosystem-Report

16. Workshop participant response, Trilateral AI Experts Group Dialogue, Melbourne, 19-20 April 2023.

17. Joseph Brookes. 2022. AI Action Plan Locked in But Changes Still Possible. 27 October, accessed 18 July, https://www.innovationaus.com/ai-action-plan-locked-in-but-changes-still-possible/

18. There is no link to a 2023 application process suggesting the foundation may be a one-time program. CSIRO – National Science Foundation (US) AI Research Collaboration Program, CSIRO, accessed 19 August, 2023 via https://www.csiro.au/en/research/technology-space/ai/NSF-AI-Research.

19. Stew Magnuson. 2023. Japan Pushing its Tech Companies to Partner with U.S. Defence Industry. National Defence, 2 June. Accessed 4 September, https://www.nationaldefensemagazine.org/articles/2023/6/2/japan-pushing-its-tech-companies-to-partner-with-us-defense-industry

20. William Greenwalt. 2019. Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies. Atlantic Council, Scowcroft Center for Strategy and Security, April. Accessed 4 September, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf

21. Daniel Kliman and Brendan Thomas-Noone. 2018. How the Five Eyes Can Harness Commercial Innovation. Defence One, 25 July. Accessed 2 August, https://www.defenseone.com/ideas/2018/07/how-five-eyes-can-harness-commercial-innovation/150040/

22. Fatima, Samar, Desouza, Kevin C., Dawson, Gregory S., & Denford, James S. (2022) Interpreting National Artificial Intelligence Plans: A Screening Approach for Aspirations and Reality. Economic Analysis And Policy, 75, pp. 378-388

23. Pernin, Christopher G., Jakub P. Hlavka, Matthew E. Boyer, John Gordon IV, Michael Lerario, Jan Osburg, Michael Shurkin, and Daniel C. Gibson, Targeted Interoperability: A New Imperative for Multinational Operations. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2075.html

24. Pernin, Christopher G., Angela O'Mahony, Gene Germanovich, and Matthew Lane, Chasing Multinational Interoperability: Benefits, Objectives, and Strategies. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3068.html

25. Royal Australian Navy. 2017. Plan Mercator: Navy Strategy 2036. Canberra, ACT: Commonwealth of Australia.

26. Ben Felton. 2022. An Inside Look at Autonomous Warrior 2022. Naval News, 6 June. Accessed 13 August, https://www.navalnews.com/naval-news/2022/06/an-inside-look-at-autonomous-warrior-2022/

27. John Christianson, Sean Monaghan, and Di Cooke. 2023. AUKUS Pillar Two: Advancing the Capabilities of the United States, United Kingdom, and Australia. Center for Strategic and International Studies, 10 July, accessed via https://www.csis.org/analysis/aukus-pillar-two-advancing-capabilities-united-states-united-kingdom-and-australia

28. Quad Critical and Emerging Technology Working Group. 16 June 2021. Australian Government Department of Foreign Affairs and Trade. Accessed via https://www.internationalcybertech.gov.au/node/137

29. Lisa Curtis, Jacob Strokes, Joshua Fitt and Andrew J. Adams. 2022. Operationalizing the Quad. Center for a New American Century, 30 June. Accessed 3 September 2023 https://www.cnas.org/publications/reports/operationalizing-the-quad

30. Guy Boekenstein. 2023. The Quad's Role in Tech Diplomacy. The ASPI Strategist, 15 February, accessed 3 September 2023 via https://www.aspistrategist.org.au/the-quads-role-in-tech-diplomacy/

31. Husanjot Chahal, Ngor Luong, Sara M Abdulla, and Margarita Konaev. 2022. Quad AI: Assessing AI-related Collaboration between the United States, Australia, India, and Japan. Center for Security and Emerging Technology, May 2022, accessed 13 August 2023, https://cset.georgetown.edu/publication/quad-ai/

32. Justin Bassi, Maeve Ryan, and Lisa Curtis. 2023. AUKUS Advanced Capabilities Pillar will Require Fundamental Shifts. The Strategist, Australian Strategic Policy Institute, 12 July. Accessed 4 September, https://www.aspistrategist.org.au/aukus-advanced-capabilities-pillar-will-require-fundamental-shifts/

33. Tom Corben, Ashley Townshend, Blake Herzinger, Darshana M. Baruah, and Tomohiko Satake. 2023.

Bolstering the Quad: The Case for a Collective Approach to Maritime Security. United States Study Centre Report, 7 June. Accessed 17 July, https://www.ussc.edu.au/bolstering-the-quad-the-case-for-a-collective-approach-to-maritime-security

34. Defence Primer: The National Technology and Industrial Base. 2023. Congressional Research Service, 30 March, accessed 5 September, https://sgp.fas.org/crs/natsec/IF11311.pdf

35. Daniel Kliman and Brendan Thomas-Noone. 2018. How the Five Eyes Can Harness Commercial Innovation. Defence One, 25 July. Accessed 2 August, https://www.defenseone.com/ideas/2018/07/how-five-eyes-can-harness-commercial-innovation/150040/

36. Stew Magnuson. 2023. Japan Pushing its Tech Companies to Partner with U.S. Defence Industry. National Defence, 2 June. Accessed 4 September, https://www.nationaldefensemagazine.org/articles/2023/6/2/japan-pushing-its-tech-companies-to-partner-with-us-defense-industry

37. William Greenwalt. 2019. Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies. Atlantic Council, Scowcroft Center for Strategy and Security, April. Accessed 4 September, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf

38. Andrew Imbrie, Daniel Baer, Andrew Trask, Anna Puglisi, Erik Brattberg, and Helen Toner. 2022. Privacy is Power: How Tech Policy Can Bolster Democracy. Foreign Affairs, 19 January. Accessed 13 August, https://www.foreignaffairs.com/articles/world/2022-01-19/privacy-power?_gl=1*12s5pob*_ga*NDE5ODIxMzUzLjE2OTM2OTQzOTg.*_

39. Defence Data Strategy 2021-2023. 2021. Australian Government Department of Defence. Accessed 4 September, https://asiapacificdefencereporter.com/wp-content/uploads/2021/08/Defence-data-strategy-1.pdf

40. Will Knight and Khari Johnson. 2023. Now That ChatGPT is Plugged In, Things Could Get Weird. Wired, 29 March. Accessed via https://www.wired.com/story/chatgpt-plugins-openai/

41. Samar Fatima, Gregory S. Dawson, Kevin C. Desouza, and James S. Denford. 2021. Winners and Losers in the Fulfillment of National Artificial Intelligence Aspirations. Brookings, 21 October. Accessed 5 September, https://www.brookings.edu/articles/winners-and-losers-in-the-fulfilment-of-national-artificial-intelligence-aspirations/

42. Justin Hendry. 2022. Defence's Enterprise-Wide Data Division Takes Shape. ITnews, 11 May. Accessed 4 September, https://www.itnews.com.au/news/defences-enterprise-wide-data-division-takes-shape-579863

www.rmit.edu.au