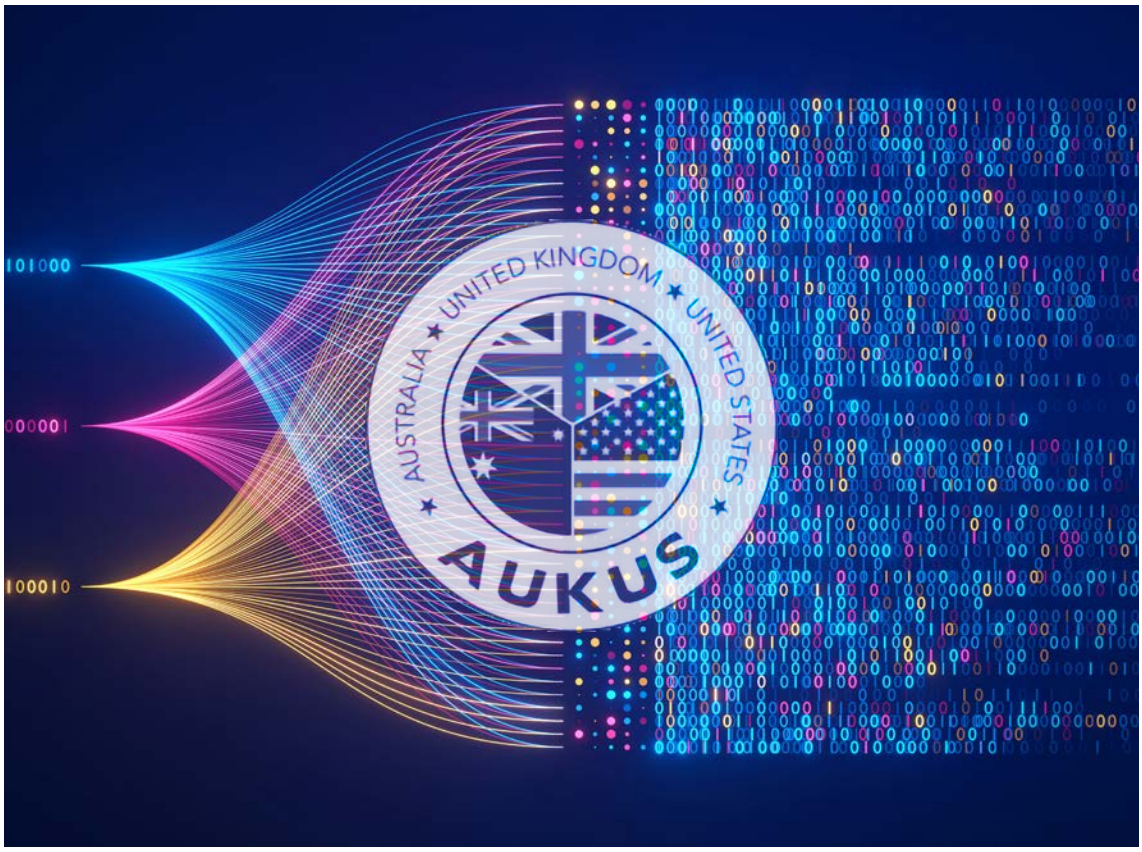
RAND AUSTRALIA

Research Report

AUSTIN WYATT, JAMES RYSEFF, ELISA YOSHIARA, BENJAMIN BOUDREAUX, MARIGOLD BLACK, JAMES BLACK

Towards AUKUS Collaboration on Responsible Military Artificial Intelligence

Co-Design and Co-Development of AI Among the United States, the UK and Australia



For more information on this publication, visit **www.rand.org/t/RRA3079-1**.

About RAND Australia

The RAND Corporation (Australia) Pty Ltd is RAND's subsidiary that does work for Australian clients on defence, national security, health, education, sustainability, growth, and development. To learn more about RAND Australia, visit www.rand.org/australia.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Canberra, Australia

Cover: NicoElNino/Adobe Stock, Australian Department of Defence..

Limited Print and Electronic Distribution Rights

About This Report

As the United States, the United Kingdom, Australia, and their close allies face rising threats from China, a key part of their strategy has been to rely on allies and partners to outpace their competitors. However, operating alongside allies and partners also comes with operational challenges and complexities. In this report, we investigate the challenges and barriers that could inhibit or prevent the co-development of artificial intelligence (AI) between the United States and its closest allies and partners. Ultimately, we identified four primary types of barriers to the co-development of AI between allies and partners: conceptual considerations, technical considerations, intellectual property considerations and ethical considerations. We make six recommendations for overcoming these potential barriers. First, the AUKUS states should continue prioritising the responsible development of AI and aligning their AI policies. Second, the AUKUS states should consider creating new joint research and development centres in which it can leverage the niche capabilities of its closest allies and partners to more rapidly advance AI. Third, to gain practical experience operationalising AI capabilities, the AUKUS states should consider integrating data analytics and AI into joint exercises that it holds with allies and partners. Fourth, the AUKUS states should consider extending its collaboration to include the co-development of operational concepts. Fifth, the AUKUS members should explore mechanisms for greater cross-sector integration of their innovation ecosystems, with a particular focus on enabling the cross-pollination of talent. Finally, the United States should consider modelling its approach to collaborating with allies and partners on its experience with Project Maven, during which the United States worked with nontraditional defence contractors in a secure unclassified environment specifically so that it could work with a broader variety of talent and expertise.

Funding

Funding for this research was provided by gifts from RAND Corporation supporters and income from operations.

About RAND Australia

RAND Australia is RAND's Canberra-based subsidiary that analyses defence, national security, economic and social issues for Australian clients. With a commitment to core values of quality and objectivity, RAND Australia combines local research talent with world-class experts from across RAND's global presence to solve complex Australian public policy problems.

For more information on RAND Australia or to contact our director, please visit www.rand.org/australia.

Acknowledgments

We thank the RAND Initiated Research Program for supporting our pursuit of this topic that is gaining recognition as an impediment to military collaboration among allies. We appreciate Nancy Staudt and Lisa Jaycox for guiding us along the way. We are grateful to our reviewers Jonathan Wong of the RAND Corporation and Carl Rhodes, Director, Inside Policy, for their thoughtful comments that improved our report.

Summary

As the United States and such close allies as the United Kingdom and Australia face rising threats from China, a key part of their strategy has been to rely on allies and partners to outpace their competitor. Collaborating with allies and partners is especially important to the advancement and adoption of artificial intelligence (AI) because it could enable the collection of greater quantities and varieties of data that are necessary to train these algorithms[1]. However, operating alongside allies and partners also comes with its own operational challenges and complexities. In this report, we investigate the challenges and barriers that could inhibit or prevent the co-development of AI between the United States and its closest allies and partners.

Ultimately, we identified four primary types of barriers to the co-development of AI between allies and partners: conceptual considerations, technical considerations, intellectual property considerations and ethical considerations. Conceptual considerations primarily concern aligning priorities and objectives within AUKUS: What is the AI project intended to achieve and how will responsibilities be divided among the partners in practice? AI is such a new technology that, although there is a consensus that it could be game-changing, there is little agreement on exactly how to begin and what AI can be reasonably expected to do. Technical considerations involve engineering factors, such as ensuring that data sets are interoperable or aligning on how to perform testing, evaluation, verification and validation on AI algorithms. Intellectual property considerations involve ensuring that the rights of all parties—militaries and private sector corporations alike—are respected both when creating these algorithms and when overcoming export control restrictions that govern how military data can be shared. The International Traffic in Arms Regulations loom especially large in this discussion. Finally, ethical considerations will need to be accounted for to ensure that the AI algorithms resulting from these collaborations are used responsibly by every partner.

To overcome these potential barriers, we make six core recommendations. First, AUKUS member states should align their approaches to prioritising the responsible development of military AI, including considering the development of a cross-national legal review process for such technologies. Second, AUKUS should coordinate the establishment of multinational research and development centres, in which the niche capabilities and skillsets of member states can be more effectively translated into meaningful technological progress. Third, AUKUS should integrate data analytics and AI into joint exercises. These should be extended beyond the AUKUS to other Five Eyes and closely allied partners. The goal should be to leverage existing exercises and mechanisms to gain practical experience operationalising these capabilities. Fourth, AUKUS members should collaborate on the development of operational concepts and shared capability goals. If this step is taken early in the technology

[1] James Ryseff, 'The United States Can Only Achieve AI Dominance with Its Allies', *War on the Rocks*, 9 October 2020.

maturation process, the amount of friction from competing operational goals could be limited and future co-deployment might be improved. Fifth, AUKUS members, particularly the United States, should consider how to better integrate each state's innovation ecosystem and enable the seamless movement of data, intellectual property and workforce between ecosystems. Finally, the United States should model its approach to collaborating with allies and partners on its experience with Project Maven, in which it worked with nontraditional defence contractors in a secure unclassified environment specifically so that it could work with a broader variety of talent and expertise. In addition to these core recommendations, we have provided a summary of challenges and supplemental recommendations, which are outlined in Tables 7.1, 7.2 and 7.3.

Contents

About This Report iii
Summary v
Chapter 1. Introduction 1
Chapter 2. Collaboration in the AUKUS Partnership 4
Chapter 3. Challenges to Collaboration 8
Ethical and Legal Considerations 8
Technical Considerations 19
Export Control Regimes 20
Meeting Distinct Operational Considerations 24
Chapter 4. Resource and Cooperation Considerations for Junior and Senior Partners 28
Chapter 5. Gathering Insights on Military Technology Collaboration 32
Concerns Raised by Policymakers and Artificial-Intelligence Experts 32
Chapter 6. Illustrative Potential Use Cases for Military AI Cooperation 42
Cyber Cooperation 43
Computer Vision 44
Chapter 7. Core Recommendations 46
Prioritise and Streamline Approaches to Ethically and Legally Responsible Artificial Intelligence 46
Create New Multinational Research and Development Centres 47
Integrate Data and Artificial Intelligence into Multinational Exercises 47
Collaboratively Develop Compatible Operational Concepts for the Use of Military Artificial Intelligence 48
Explore Mechanisms for Greater Innovation Ecosystem Integration 49
Implement the 'ITAR-Free Zone,' or the Maven Model 49
Abbreviations 53
References 54

Tables

Table 7.1. Challenges and Recommendations: Leverage Strengths of Each Partner While Preserving the Perspective and End Value of the Product to Junior Partners 51
Table 7.2. Challenges and Recommendations: Developing and Integrating Ethically and Legally Responsible Artificial Intelligence 52
Table 7.3. Challenges and Recommendations: Practical Aspects of Enabling Cooperation Across Barriers 52

Chapter 1. Introduction

Artificial Intelligence (AI) technologies stand to play a prominent role in defence applications, varying from back-office enterprise services that supporting military personnel and procurement, to cyber and information operations, to warfighter functions on the battlefield. Militaries around the world seek to leverage AI technologies, which has increased competition between states striving for strategic and operational advantages.

One key source of strength for the United States, Australia and the United Kingdom (UK) in this competitive environment is that they regularly operate within a coalition of countries that working together offer opportunities beyond what any state can do on its own. Multinational coalitions expand the reach and strength of military forces and can leverage comparative advantages in technologies and other areas that can promote deterrence and improve battlefield outcomes.

The 2021 trilateral agreement between Australia, the UK and the United States—known as AUKUS—will be important across multiple areas of security cooperation. Per a statement from, the Joint Leaders, the goal of AUKUS is to form a 'new security partnership that will promote a free and open Indo-Pacific that is secure and stable', in part by providing Australia with nuclear-powered submarines.[2] In addition, AUKUS seeks to pioneer new forms of collaboration and interoperability in emerging technologies, such as AI.[3] Because the agreement is between three close partners and is significantly smaller than the North Atlantic Treaty Organization (NATO) and other arrangements, AUKUS could have the flexibility and cohesiveness to build multinational approaches to emerging technologies. Once there is a model for AI and other emerging technology collaboration in this smaller alliance, these mechanisms and concepts might then be leveraged for broader coalitions.

The co-development of AI holds great promise for AUKUS for several reasons. For one, co-developing AI algorithms allows each of partner to increase the quantity and quality of data its algorithms are trained on.[4] U.S. software companies have long leveraged the data acquired from their global dominance to maintain an advantage over their Chinese counterparts in the commercial space.[5] However, this advantage is offset by the fact that China has been able to leverage its scale and ability to compel businesses and citizens to hand

[2] White House, 'Joint Leaders Statement on AUKUS', 13 March, 2023.

[3] The 'Advanced Capabilities' in Pillar Two of AUKUS are: undersea capabilities; quantum technologies; AI and autonomy; advanced cyber, hypersonic and counter-hypersonic capabilities; and electronic warfare (John Christianson, Sean Monaghan, and Di Cooke, *AUKUS Pillar Two: Advancing the Capabilities of the United States, United Kingdom, and Australia*, Center for Strategic and International Studies, 2023).

[4] Erik Lin-Greenberg, 'Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making', *Texas National Security Review*, Vol. 3, No. 2, Spring 2020.

[5] Ryseff, 2020; Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence*, W.W. Norton & Company, 2023.

over vast swathes of data.[6] Cooperation between the United States and its closest allies has been pushed as a mechanism for re-establishing Western dominance in AI for the military sphere. Additionally, co-developing AI would expand the pool of technical talent available to work on these difficult problems[7]. Finally, co-developing military applications of AI could deepen relationships between allies and partners and help build enduring military advantages that ensure that democratic governments around the world maintain a technical advantage over their potential opponents.

However, there are major challenges associated with finding a path for collaboration in military AI, even among close allies, such as AUKUS. The first of these challenges is how to best leverage the strengths of each partner while preserving the perspective and end-value of the product to junior partners. Because of their substantially smaller military and economic capacities, Australia and, to a lesser extent, the United Kingdom are the junior partners in Pillar Two. Given the significant resource capacity advantage of the United States, there is an understandable risk that its interests overtake those of junior partners in the design of collaborative AI projects. However, a key aspect of the value proposition of AUKUS is pooling talent among partners by leveraging niche capability areas in which Australia and the UK have secured an advantage. Measuring input value in purely monetary or scale terms or allowing U.S. primes to monopolise the development process wastes those advantages. Strong leadership is equally necessary for securing a meritocratic division of effort and equitable access to the end product; junior partners cannot be reduced to silent partners. Finally, it has historically been difficult for states to ensure that a co-developed system meets their requirements, including visibility into how the system operates, freedom to domestically modify the system, supply chain security risks and life of type support costs (which could be quite distinct or even mutually exclusionary). AUKUS needs to find a path that balances compromise with capability between a superpower, a regional great power and the quintessential middle power.

The second key challenge is that the three members of AUKUS and many other countries are still evaluating how AI can be integrated into military applications, as well as how it might be integrated *responsibly*. While each AUKUS state has released some variety of Defence AI strategy and ethics statement, these policies are early in the implementation phase. This status leaves a level of uncertainty as to how emergent norms for responsible use will be integrated in how AI capabilities are developed, tested and evaluated for vulnerabilities and risk, and how to ensure that rapidly developing AI operates as intended. There might also be divisions between states about how the role of human judgment, oversight and control over AI capabilities. These aspects could be crucial in potentially lethal applications of AI, such as the use of autonomous weapons.

The final major challenge relates to the practical aspects of enabling cooperation between militaries across traditionally stringent barriers. For example, existing restrictions on the

---

[6] Scharre, 2023.

[7] Bhaskar Chakravorti, Ajay Bhalla, Ravi Shankar Chaturvedi and Christina Filipovic, '50 Global Hubs for Top AI Talent', *Harvard Business Review*, 21 December 2021.

export of military technologies, most notably from the United States (including International Trafficking in Arms Regulations [ITAR]), might also affect whether allies can acquire technologies that will enable them to leverage comparative advantages. These restrictions have significant sovereignty implications that affect the security of supply, freedom of action, affordability and future option space for states that want to collaborate with the United States. Other practical barriers include differences in operational concept and doctrine, the risks of relying on a system that was taught using a different set of ethical or legal standards and the problem of accountability in wartime.

Because of the potential opportunities of AUKUS and the complexities of cooperating on emerging AI technologies, this report addresses the question of how the United States, UK and Australia can work together to co-design and co-develop military AI capabilities. This question requires the consideration of key legal and ethical elements and technical barriers to collaboration.

This report is structured as follows. First, we provide additional background on AUKUS, particularly the relevant Pillar Two component focused on emerging technologies. We then discuss some of the challenges associated pursuing collaboration under AUKUS, first by discussing each country's approach to responsible and ethical AI deployment (including discussion of their respective weapons review processes) and then by discussing technical barriers that might hinder interoperability. We also consider how export controls on the U.S. side could especially complicate or prevent certain forms of collaboration.

To break through these barriers and move forward, we consider several case studies of multinational military cooperation and identify some lessons for AUKUS collaboration on military AI. These case studies are supported by a detailed open-source scan of government, scholarly and grey literature.[8] We focused on prominent academic journals, think tank–associated reports and government press releases. A notable majority of these sources emanated from Australia, which reflects the importance that AUKUS has secured in Australia's defence thinking. Another prominent theme that we identified in our scan of the literature was the importance of overcoming the challenges on collaborative development imposed by the current defence export restriction frameworks, particularly ITAR. We conclude by offering a set of recommendations to develop shared approaches, adapt existing fora and conduct new activities to further improve the AUKUS partnership.

[8] Papers were identified chiefly through use of the RAND Knowledge Services database, Scopus and Google Scholar. Keywords included (in varying combinations): 'autonomous weapon systems', 'military co-development', 'AUKUS', 'ITAR', 'export control', 'military artificial intelligence' and 'ethical challenges of LAWS'.

Chapter 2. Collaboration in the AUKUS Partnership

The collaborative aspects of the AUKUS agreement are of paramount importance to the success of its technological dimensions. In this sense, the AUKUS agreement exemplifies recognition of the need to reevaluate, restructure and invigorate alliance relationships through the combination of information-sharing and capability-building.[9] The agreement fits into the UK's broader tilt towards the Indo-Pacific following its Integrated Review,[10] and builds the UK's bilateral relationships with Australia and the United States independent from NATO and Europe.[11] From the U.S. perspective, AUKUS coordinates with its recognition that it will need capable allies and partners in competition with China, aligns with its increasing military presence in the region, and supports co-deployment capability with the Australian Defence Forces (ADF).[12] The establishment of a rotational forward deployment of U.S. submarines at HMAS Stirling, an Australian naval base, (referred to as *Submarine Rotational West*) also offers significant strategic advantages.[13] These advantages are imperative in the context of the growing technological sophistication and advancement of China and other authoritarian regimes in eroding U.S. primacy and advantage, particularly in such fields such hypersonics and AI, and the risk that nonstate actors will leverage disruptive new technological capabilities to threaten the United States and its allies.[14] In the present geopolitical moment, the importance of technological leadership and alliance partnerships in the exercise of state power is evident.[15] AUKUS countries have found themselves with a declining relative power;[16] their defence innovation systems have suffered relative stagnation after the Cold War, 'while technological progress is now driven across a globalised commercial industrial base'.[17]

[9] Thomas Corben, 'A Year On—What to Make of AUKUS After 365 Days?' Royal United Services Institute of New South Wales, 23 November 2023, p. 13.

[10] The Integrated Review 2021 was a UK Ministry of Defence strategic refresh that articulated the UK's strategic national interests as centered around sovereignty, security and prosperity (UK Cabinet Office, 2021).

[11] Peter Jennings, *AUKUS: New Opportunities for the United States and its Closest Allies*, Heritage Foundation, 18 October 2022.

[12] Jennings, 2022.

[13] Ashley Townshend, 'The AUKUS Submarine Deal Highlights a Tectonic Shift in the US-Australia Alliance', Carnegie Endowment for International Peace, 27 March 2023.

[14] William Greenwalt and Tom Corben, *Breaking the Barriers: Reforming US Export Controls to Realise the Potential of AUKUS*, United States Studies Centre at the University of Sydney, 2023, pp. 5, 7.

[15] Justin Bassi, 'Why the AUKUS Partnership Is About Much More Than Warfighting', *The Hill*, 23 October 2023.

[16] Jennifer Jackett, *Defence Innovation and the Australian National Interest*, Defence and Security Institute University of Western Australia, 2023.

[17] Greenwalt and Corben, 2023, p. 5

Increasingly, the technologies required to counter contemporary threats are being led by the commercial markets.[18] As a result, research, products and practices are more broadly available to allies and opponents alike. New efforts and initiatives are thus needed to maintain a technological edge, particularly as some countries, such as China, are surging ahead in this respect.[19] AUKUS is a means by which to remediate this potential gap; it is a reaction to the 'collision of geopolitics with technology policy'.[20] This anglophone grouping symbolises the prioritisation of resilience,[21] and a collective approach to defence innovation from allies and partners in recognition of underperformance in their collective military capabilities in deterring 'Chinese adventurism and potential military action in the near- to medium-term future'.[22] The formation of AUKUS was driven by an urgent need to develop 'new asymmetric, disruptive defence capabilities by the countries pursuing this collective strategy of deterrence'.[23] In this sense, AUKUS is meant to symbolise a restructuring of alliance parameters to capitalise on allied offerings from states that were once seen as junior partners in the technological space. Australia and the UK are no longer to be seen as 'passengers' of U.S. technological primacy but 'increasingly important sources of innovation and cutting-edge technology in their own right'.[24] This shift means that 'AUKUS partners need to understand areas of comparative advantage, complementarity, and potential gaps or overlaps, between the three industrial bases'.[25] The partner states can do so by uplifting capacity for technical interoperability and exchange and building more ambitious partnerships in industry (e.g. around nuclear submarines).[26] These steps require removal of any obstructions to technology and information transfer and to combined capability and workforce development. The intent is the development of an industrial strategy and a technology control-system that are effectual across the United States, Australia and the UK.[27]

While AUKUS is a relatively recent initiative in terms of technological cooperation between the countries, it builds on and complements existing bilateral and multilateral

---

[18] James Ryseff, Eric Landree, Noah Johnson, Bonnie Ghosh-Dastidar, Max Izenberg, Sydne Newberry, Christopher Ferris and Melissa A. Bradley, 'Exploring the Civil-Military Divide over Artificial Intelligence', RAND Corporation, RR-A1498-1, 2022.

[19] Jamie Gaida, Jennifer Wong-Leung, Stephanie Robin and Danielle Cave, *ASPI's Critical Technology Tracker: AUKUS Updates*, Australian Strategic Policy Institute, last updated 22 September 2023; William Greenwalt, *Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies* , Scowcroft Center for Strategy and Security, 2019, p. 18.

[20] Jackett, 2023, p. 9.

[21] Jackett, 2023, p. 9.

[22] Greenwalt and Corben, 2023, p. 5

[23] Greenwalt and Corben, 2023, p. 5

[24] Greenwalt and Corben, 2023, p. 3.

[25] Jennifer Jackett, *Laying the Foundations for AUKUS: Strengthening Australia's High-Tech Ecosystem in Support of Advanced Capabilities*, United States Studies Centre at the University of Sydney, 2022, p. 2 .

[26] Christianson, Monaghan and Cooke, 2023.

[27] Greenwalt and Corben, 2023, p. 46.

efforts.[28] AUKUS contributes to the goal of these existing efforts to grow 'the connective tissue' between likeminded, democratic partners.[29] AUKUS collaboration would complement Australian and U.S. membership in the U.S. National Technology and Industrial Base and the Five Eyes Technical Cooperation Program.[30]

AUKUS builds on these initiatives and programs but offers some degree of novelty or new momentum in its purposive approach to developing the structural dimensions of technological collaboration. This approach is reflected in the importance of technological collaboration to both Pillar One and Pillar Two of the AUKUS agreement. The former focuses on the provision of conventionally armed, nuclear powered submarines to Australia; the latter focuses on 'trilaterally developing and providing joint advanced military capabilities'.[31] If there is cognisance of driving questions, such as what each party provides in the development of a collective military technological edge or how the alliance fills respective critical capability gaps, AUKUS offers enormous potential to advance cutting-edge capabilities,[32] particularly because advancement in one capability stream 'will also act as an enabler and force multiplier for other advanced capabilities'.[33]

For Pillar Two, specifically, there is recognition that the AUKUS partnership could be 'more urgent' and indeed, more opportune and substantive in the benefits it might offer to partners.[34] Advancements in quantum, cyber, AI, undersea, hypersonics and electronic warfare should offer advantages across military and economic contexts.[35] Benefits could extend to broad-based linking of 'our defense industrial bases, integrating our defense supply chains, and co-producing key technologies that will shore up our collective military advantages',[36] which reflects a focus on 'uplift[ing] . . . the science, technology and industrial ecosystems of all three countries'.[37]

Particularly in the context of Pillar Two technologies, AUKUS relies on not only the defence industrial base but also the broader innovation ecosystem for dual-use technologies, such as AI. There is an interdependency between technological development in a general sense and military-specific technological advancement, especially in the current landscape. As a result, there must be recognition of how to harness—in Australia, for example—'existing strengths in areas like research and talent, and its growing technology sector, and

---

[28] These efforts include the 1958 U.S.-UK Mutual Defence Agreement, the 2007 U.S.-Australia Defense Trade Treaty and AUSMIN Defence Acquisition Committee (Brendan Thomas-Noone, *Tech Wars: US-China Technology Competition and What It Means for Australia*, United States Studies Centre at the University of Sydney, 2020).

[29] White House, *National Security Strategy 2022*, October 2022b, p. 11.

[30] Corben, 2022, p. 13. See Australian Department of Defence, 'The Technical Cooperation Program', webpage, undated.

[31] Christianson, Monaghan and Cooke, 2023.

[32] Christianson, Monaghan and Cooke, 2023.

[33] Jackett, 2022.

[34] Jackett, 2022, p. 4.

[35] Christianson, Monaghan and Cooke, 2023.

[36] White House, *Indo-Pacific Strategy of the United States*, February 2022a, p. 13.

[37] Jackett, 2022, p. 4.

build on existing areas of advantage in the defence sector specifically, like in manufacturing of naval and aerospace components'.[38]

A broad conceptualisation of the innovation space—and commensurate reevaluation of the processes, structures and regulations such that the alliance can move at a 'speed of relevance'—are central to successful collaboration.[39] The U.S. Assistant Secretary of State for Political-Military Affairs stated that a 'top priority is to create new and open ways to share information and technology' with the AUKUS partners.[40] However, AUKUS is two years old, and these architectures are not yet in place. In the absence of effective mechanisms for overcoming these entrenched organisational barriers, there is a real risk that AUKUS will remain hampered by the same legal, political, structural and regulatory obstructions that have frustrated the ambitions of prior attempts at U.S.-UK-Australian technological cooperation. While AUKUS might successfully allow for acceleration, it will not be able to fulfill its potential to 'diversify or multiply' as hoped without overcoming organisational barriers.[41]

[38] Jackett, 2022, p. 12

[39] Jackett, 2022.

[40] Jessica Lewis, 'Modernizing U.S. Arms Exports and a Stronger AUKUS', testimony before the House Committee on Foreign Affairs , U.S. Department of State, 24 May 2023.

[41] Corben, 2022, p. 15.

Chapter 3. Challenges to Collaboration

In this chapter, we consider various challenges to AUKUS collaboration on the co-development and co-design of AI.

Ethical and Legal Considerations

Artificial-Intelligence Ethics Principles

The extent to which AUKUS partner countries have a shared understanding of the ethical use of AI in a military context provides important insight into the potential opportunities and challenges of co-designing and developing responsible AI capabilities. The United States, UK and Australia have each developed a set of ethical principles on the use of AI in military applications specifically (United States and UK) or more broadly (Australia).[42] Although there is significant alignment across the AUKUS partners on these principles, there is also a significant amount of ambiguity in how the principles will be implemented and operationalised, which could negatively affect the partners' shared strategic objectives related to responsible military AI.

In general, the AUKUS countries endorse a set of shared ethical principles on AI, particularly with regards to

- **minimising bias and discrimination** by addressing the potential discriminatory outcomes of AI systems
- **ensuring explainability** by establishing mechanisms for auditing AI systems despite their black-box nature and equipping relevant personnel with an appropriate level of understanding of those systems
- **establishing accountability** by identifying and assigning responsibility for AI systems and their outcomes throughout a system's life cycle
- **ensuring human control** by requiring human oversight over the use of AI systems
- **promoting reliability** by ensuring that AI systems operate as intended (e.g. through continual testing and monitoring), the ability to disengage or deactivate deployed systems that demonstrate unintended behaviour and the use of hardware and software to prevent unauthorised users from tampering with a system.[43]

There is also general alignment across these governments on the development and use of a particularly sensitive subclass of military AI: lethal autonomous weapons. Since 2014, 84 states (including the United States, the UK and Australia) have participated in United Nations discussions at the Convention on Conventional Weapons on Lethal Autonomous

[42] Australian Department of Industry, Science and Resources, *Australia's Artificial Intelligence Ethics Framework*, 7 November 2019; DoD, 'DOD Adopts Ethical Principles for Artificial Intelligence', press release, 24 February 2020; UK Ministry of Defence, *Ambitious, Safe, Responsible: Our Approach to the Delivery of AI-Enabled Capability in Defence*, 2022;

[43] We generated this list using an analysis of these ethical frameworks.

Weapon Systems (LAWS). Discussion in that forum has centred on various ethical questions posed by LAWS, including the definition and risks of LAWS, the role of humans in the exercise of force, and whether there is a need for new international regulatory mechanisms. As part of these discussions, the three AUKUS partners have collaborated and endorsed various statements and proposals on LAWS, including a set of 'Guiding Principles', which generally reflect the principles laid out in the partners' respective national ethical frameworks.[44] In May 2023, the three partners—along with Japan, South Korea, Canada and Poland—issued a set of draft articles that specified 'prohibitions and other regulatory measures' under existing international humanitarian law (IHL) that are applicable to LAWS.[45] On the 22nd of December 2023, each AUKUS state voted for the passage of UN General Assembly Resolution 78/241, which acknowledged that "serious concerns" stemming from LAWS and requested that the Secretary General seek the views of member states toward a report (due September of 2024) on how to address ethical, legal and humanitarian risks.[46] While all three AUKUS members voted for the resolution, it is notable that 78/241 is only an initial step. Support for the resolution reflected the general agreement across the AUKUS partners that the design and development of autonomous weapon systems should be controlled but not banned and that human discretion and oversight of the broader targeting *process* (for example, through legal reviews and determining the appropriate temporal and geographic parameters of a system prior to its deployment) rather than the specific *act* of engaging a military target with kinetic force sufficiently complies with the principle of human control and states' obligations under IHL more broadly.[47]

While there is considerable alignment across the AUKUS partners on many of the foundational ethical principles, there are some areas in which the United States, the UK, and Australia could benefit from additional discussion around what it means to employ AI responsibly in a military context. For example, U.S Department of Defense (DoD) guidance does not explicitly include the following principles, which have been endorsed by either the UK, Australia, or both as part of their ethical frameworks: **protection of people, society and the environment**; **privacy**; and **transparency**.[48] In addition, compared with those of the United States, UK and Australian ethical principles and guidance contain more-robust discussions of **minimising bias and discrimination** and **establishing accountability**. For example, while all three partners touch on the importance of minimising bias and discrimination in the use of AI systems, the UK and Australia include examples of specific steps for ensuring that bias is minimised, such as addressing bias in algorithmic

---

[44] United Nations, *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, September 2019.

[45] Australia, Canada, Japan, Republic of Korea, United Kingdom and United States, *Draft Articles on Autonomous Weapon Systems—Prohibitions and Other Regulatory Measures on the Basis of International Humanitarian Law ('IHL')*, United Nations, 13 March 2023.

[46] United Nations, Lethal Autonomous Weapon Systems, General Assembly Resolution 78/241, 12 October 2023.

[47] Australia Canada, Japan, Republic of Korea, United Kingdom and United States, 2023.

[48] Australian Department of Industry, Science and Resources, 2019 ; DoD, 2020; UK Ministry of Defence, 2022.

decisionmaking (UK) and consulting with stakeholders (Australia).[49] Furthermore, all three partners discuss the need to establish human and organizational responsibility for AI systems, but the United States broadly posits that 'DoD personnel' are responsible for AI systems,[50] while the UK and Australia go further by clarifying that the organization or individual responsible for a system or its outcomes should be clearly identifiable. In its AI ethical principles, Australia further specifies that AI systems should be subject to external review and that there should be grievance mechanisms in place for individuals to challenge decisions made by or with the support of these systems.[51] Neither of these mechanisms is particularly applicable in the case of LAWS, in which IHL would be relied on to enforce accountability.

Significant questions remain as to how each country will implement their established ethical principles, either alone or in coordination with partners and allies. The United States and the UK have established policies on military AI and autonomous weapons, more specifically. These policies outline the roles, responsibilities and principles related to the governance of military AI. In contrast, Australia does not have a defence policy that specifically deals with the military applications of AI. Even in the case of the U.S. and UK military AI policies, there is significant ambiguity around the operationalization of the ethical principles. For example, the DoD Directive 3000.09, *Autonomy in Weapon Systems*, requires the Secretary of Defense for Research & Engineering (USD R&E) and Chief Digital and Artificial Intelligence Officer (CDAO) to 'formulate concrete, testable requirements for implementing the DoD AI ethical principles'.[52] However, the directive does not further specify how a system's design, testing requirements, or use would or would not comply with those principles. As of November of 2023, it does not appear that the USD R&E or CDAO have implemented additional guidance that would help clarify this ambiguity. Similarly, the UK Ministry of Defence's 'Ambitious, Safe, Responsible' policy on AI-enabled capability in defence states that the 'appropriate degree of system 'autonomy' and type of 'human control' needs to be considered carefully on a case-by-case basis', but does not further delineate how this principle could be applied to different types of weapon systems, domains of warfare, or operational contexts.[53]

In February 2023, the U.S. Department of State issued a *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, which broadly reaffirms U.S. ethical principles on the use of AI in military applications.[54] Specifically, the declaration encourages 'endorsing states' to ensure that relevant personnel exercise 'appropriate levels of human judgement', that steps are taken to minimise unintended bias and that AI capabilities are subject to 'rigorous testing and assurance' across their life cycle. In interviews, State

[49] Australian Department of Industry, Science and Resources, 2019; UK Ministry of Defence, 2022.

[50] DoD, 2020.

[51] Australian Department of Industry, Science and Resources, 2019.

[52] DoD, *Autonomy in Weapon Systems*, DoD Directive 3000.09, 25 January 2023.

[53] UK Ministry of Defence, 2022.

[54] U.S. Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, 2023.

Department officials explained that they view the declaration as a mechanism for building consensus among countries around the appropriate use of military AI and for creating guardrails as this technology becomes more diffuse across countries with varying capabilities and strategic objectives.[55] However, these officials also acknowledged that efforts around defining the parameters of responsible military AI are relatively nascent and that more work needs to be done to clarify how the principles will be operationalised.

Reducing the ethical risks of an AI system not only helps to ensure that the system is employed responsibly in accordance with international humanitarian principles, doing so also improves the system's military utility. A system that is unreliable and does not behave as a commander or operator expects on the battlefield creates serious risks. A system with biased or unexplainable outcomes will quickly lose taxpayer support. Broad agreement among the AUKUS partners on AI ethical principles provides a unique opportunity to leverage shared values to achieve positive operational outcomes, but these benefits might not be realised without a concerted, coordinated effort to clarify the ethical principles and their implementation more fully. Particularly in the context of such initiatives as the U.S. declaration aimed at achieving alignment across a diverse group of countries with potentially competing priorities, it will become even more important for AUKUS partners to work towards minimising opportunities for misinterpretation of the ethical principles and to establish clear and open channels for sharing challenges and lessons learned with regards to the implementation of these principles.

Operationalising International Humanitarian Law: Article 36 Legal Review Processes

Under the current international legal framework, responsibility is assigned to individual states ensure that their means and methods of warfare do not offend the principles of IHL. Quite aside from the question of whether Article 36 legal review processes are an effective mechanism for regulating emergent autonomous systems, there are serious questions being raised in the international discourse as to whether such responsibility should remain with individual states.[56] This concerns stems from the fact that there is neither an internationally set process for undertaking such reviews nor an independent authority that could audit inadequate or inappropriate processes.

Because Article 36 imposes a broad obligation to conduct a review without mandating the contents of the review, individual states choose how to meet the obligation. By comparing the approaches of leading international arms developers and importers, Boulanin and Verbruggen were able to identify three steps that are generally reflected in Article 36 legal review

[55] U.S. Department of State officials, interviews with authors, May–August 2023.

[56] This refers to a requirement under Article 36 of Additional Protocol 1 of the Geneva Convention that requires contracting parties to conduct a review of any 'study, development, acquisition or adoption of a new weapon, means or method of warfare' to determine whether it would be prohibited by IHL (International Committee of the Red Cross, 'Article 36—New Weapons', webpage, undated).

processes.[57] Areas for collaboration and deconfliction for conducting legal reviews of future co-developed systems can be identified from these similarities.

The first step is to make an initial decision as to whether the weapon system and/or mechanism for its employment is already 'prohibited or restricted by a treaty' ratified by the state or by customary international legal principles.[58] In the most straightforward sense, this entails the responsible officer certifying that the innovation does not fall foul of a preexisting restriction or prohibition. This step is followed by a consideration of whether the weapon systems cause 'superfluous injury or unnecessary suffering', that are inherently indiscriminate, or that are 'intended, or may be expected, to cause widespread, long-term, and severe harm to the natural environment'.[59] Finally, there is a consideration of the Martens Clause, a stopgap provision to ensure restrictions on systems that are not covered by the Additional Protocol One criteria but still offend the 'principles of humanity' and 'dictates of public conscience'.[60]

Reflecting their different engagements with established IHL, the United States, UK and Australia have adopted distinct approaches to conducting Article 36 reviews. While each approach includes some variation of the common steps identified by Boulanin and Verbruggen, there are also differences that could complicate future co-development efforts, especially in the absence of specific international prohibitions on LAWS.

Australia

Australia has largely sided with the United States and the UK in pushing national-level regulation rather than a ban under IHL. However, it was one of the earliest states to publish its approach to Article 36 legal review processes at a meeting of the Group of Governmental Experts on LAWS at the United Nations.[61] As a result, there is significant detail on Australia's requirements and processes in the public domain.

Within the Australian Department of Defence, the responsibility for undertaking legal reviews falls within the Directorate of Operations and Security Law (DOSL), which is part of Defence Legal Division. In addition to managing the reviews, DOSL's mission includes the retention and expansion of 'corporate knowledge and experience' on

- Australian legal positions (i.e. based on weapons law Treaties, accepted common international law [CIL]), weapons law practices, weapons development and employment;

---

[57] Vincent Boulanin and Maaike Verbruggen, *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies*, Stockholm International Peace Research Institute, 2017.

[58] Boulanin and Verbruggen, 2017, p. 4.

[59] Boulanin and Verbruggen, 2017, pp. 1, 22.

[60] The Martens Clause is a failsafe clause in IHL that prohibits those means and methods of warfare that do not violate a specific principle of IHL yet offend the principles of humanity and the dictates of public conscience (Diego Mauri, 'The Holy See's Position on Lethal Autonomous Weapons Systems: An Appraisal Through the Lens of the Martens Clause', *Journal of International Humanitarian Legal Studies*, Vol.11, No.1, 2020).

[61] 'The Australian Article 36 Review Process', Second Session, *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious*, 27–31 August 2018.

- the operation of weapons (i.e. historical weapons use, extant order of battle, technical specifications, current strategy and methodology for use, functionality);
- weapons data (i.e. data capture points, requisite assessable data, data interpretation, application of data to specifications, relevance of performance standards and reliability to legal obligations, insufficient data processes);
- ballistic information (i.e. ballistics data, analysis and assessment, wound ballistics methodology); and
- awareness of and access to subject matter experts.[62]

As part of its independent function, the DOSL operates outside the traditional chain of command within the Department of Defence. It is staffed with a combination of senior defence and civilian lawyers who have experience undertaking military legal reviews. In addition, DOSL lawyers seek input and guidance, particularly on technical details, from other government departments and subject-matter experts. They can also draw on the Attorney General's Department, the Department of Foreign Affairs and Trade, and the Australian Government Solicitor for guidance and support.[63]

However, it is the relevant project manager who bears the responsibility to request a review. Project managers are required to request an Article 36 legal review for cases in which their project involves the development, acquisition or adoption of a new weapon system or the 'adaption or modification' of an existing system.[64] Among the DOSL's responsibilities is educating Defence decisionmakers on when it is appropriate to request a review. Guidance is also contained in the Defence procurement head policy document, the *Capability Life Cycle Manual*.[65]

Once the need has been identified by the project manager, the DOSL will assign a review team. Generally, these review teams are led by two lawyers. The first is a 'Legal Reviewer' (typically either a O4–O5 grade military lawyer or the civilian equivalent), who conducts the initial review. This document is then assessed by a more senior lawyer (O6 or civilian equivalent).[66] For simple cases, in which 'the study, development, acquisition or adoption is simple, expedited or otherwise limited in scope', this the entire process.[67] Examples of when this might be appropriate would be when a rapid operationally vital procurement methodology is utilised, or when a new use for an existing weapon system or a novel doctrine for its employment is devised.[68] The process becomes more extensive in sensitive or complex technologies, which autonomous weapon systems will almost certainly be. In such cases, a multistage version of the process is undertaken by a multidisciplinary panel. This panel might

---

[62] 'The Australian Article 36 Review Process', 2018.

[63] 'The Australian Article 36 Review Process', 2018.

[64] 'The Australian Article 36 Review Process', 2018.

[65] 'The Australian Article 36 Review Process', 2018.

[66] 'The Australian Article 36 Review Process', 2018.

[67] 'The Australian Article 36 Review Process', 2018.

[68] Australian Department of Defence, *Defence Legal Review of New Weapons Guide*, 2020.

issue several iterative interim reports.[69] The final output report is an extensive document that details, among other things, the technical specifications, testing and verification data and analysis, and a review of its legality under international law.[70]

Regardless of which mechanism is used to undertake the review, the Australian Department of Defence clearly lists six criteria covered by an Article 36 legal review in their 2018 submission:

> Whether the capability is a weapon, what the normal use of the system is intended to be (at the time of the evaluation), evaluation of the technical specifications, and whether utilizing the system is contrary to the public interest, principles of humanity or the dictates of public conscience (essentially an expanded reading of the Martens Clause).[71]

At the core of these criteria is whether there is a specific prohibition against the proposed system or, if not, whether it would be subject to general prohibition as a result of violating the tenets of IHL.[72] This final criteria also requires consideration of whether the system is 'likely to be affected by current or possible future trends in the development of international humanitarian law'.[73] How this is being interpreted in the context of a potential ban on autonomous weapon systems is currently unclear.

Under the Australian system, an Article 36 legal review can lead to three outcomes. The system can be given full clearance, it can be denied clearance or it can be granted clearance with certain conditions or limitations. These restrictions could be technical, legal or operational, and are typically designed in consultation with subject-matter experts and the program manager.[74]

United Kingdom

The process in the United Kingdom system is roughly comparable. The lead agency for conducting weapon legality reviews is the Development, Concepts and Doctrine Centre (DCDC).[75] The DCDC is a tri-service think tank that operates under Joint Forces Command independent on the single service chain of command. Essentially, the DCDC the doctrinal counterpart of the Defence Science and Technology Laboratory. Its legal component is

---

[69] Australian Department of Defence, 2020.

[70] Australian Department of Defence, 2020.

[71] 'The Australian Article 36 Review Process', 2018.

[72] Specifically, whether the system is:

- of a nature to cause superfluous injury or unnecessary suffering.
- capable of being used discriminately;
- capable of being used proportionately;
- expected to cause widespread, long term and severe damage to the natural environment.

[73] 'The Australian Article 36 Review Process', 2018.

[74] 'The Australian Article 36 Review Process', 2018.

[75] Development, Concepts and Doctrine Centre, *UK Weapon Reviews*, 2016.

staffed by experienced lawyers on three-year rotations from the single service legal divisions.[76]

Under the UK system, the DCDC conducts legal reviews at three points in the acquisition cycle: the 'initial gate' (when funds are allocated), the 'main gate' (where the DoD commits to procuring the equipment) and the date when it enters service.[77] In cases in which the procurement is conducted under the 'Urgent Capability Requirements' framework, this process is compressed, although a more comprehensive follow-on review is required.[78] It is worth noting that in the limited cases in which a decision is taken not to undertake a review, DCDC is mandated to undertake a review if the system is utilised in a new manner or upgraded.[79]

Once it is determined that a review is required, a lawyer is assigned from DCDC to conduct it. In addition to monitoring the development process, this lawyer is responsible for undertaking the draft review in consultation with the procurement team.[80] The review considers a wide variety of information, including international treaties, scholarly research and information from manufacturer. They can also request additional tests and evaluations and will draw on consultations with government and nongovernment experts.[81] The draft review is then checked by the procurement team to ensure that the lawyer has not made any technical errors related to the technology. The final step in the process is two written peer reviews by other senior DCDC lawyers. The result of this process is formal written legal advice that is placed on file.[82]

United States

There are two initial differences in the approach that the United States takes to legal reviews. First, it has no single procedure that it mandates must be followed, other than that it be conducted by an 'authorised attorney'.[83] Second, the United States is not a party to Additional Protocol One,[84] and is thus not officially bound by its Article 36.[85] This is significant because the United States would not necessarily be bound by restrictions

---

[76] DCDC, 2016.

[77] DCDC, 2016.

[78] DCDC, 2016.

[79] Boulanin and Verbruggen, 2017.

[80] DCDC, 2016.

[81] DCDC, 2016.

[82] DCDC, 2016.

[83] Boulanin and Verbruggen, 2017.

[84] Additional Protocol I to the Geneva Convention came into force in December 1978. It is the foundational document in IHL, from which we derive the modern legal requirements for conduct of hostilities. Among other aspects of the laws of war, Additional Protocol 1 mandates that militaries follow the principles of distinction, proportionality and military necessity.

[85] Article 36 of Additional Protocol I to the Geneva Convention imposes a requirement to conduct a review of all new weapons, means or methods of warfare to ensure that their use would not be prohibited by existing international law; Boulanin and Verbruggen, 2017.

emplaced on autonomous systems under Additional Protocol One, while the UK and Australia would be. Instead, the United States has imposed on itself a legal review requirement under a series of policies since 1974. For example, DoD Instruction 5500.15 requires 'legal review' of all weapons to ensure that 'their intended use . . . is consistent with . . . the laws of war'.[86] DoD Directive 2060.1 requires all DoD activities to comply with arms control agreements to which the United States. Is a party.[87] Of direct relevance to military AI and autonomous systems, DoD Directive 3000.09 imposes a requirement to exercise 'appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement',[88] and that such systems 'must be reviewed and approved by the Under Secretary of Defense for Policy, the Under Secretary of Defense for Research and Engineering, and the Vice-Chairman of the Joint Chiefs of Staff before they are formally developed, and again before they are fielded'.[89]

Within this policy framework, each service branch adopts its own approach to conducting legal reviews. In the case of the U.S. Army, a single lawyer is assigned to undertake the review, although they have broad authority to request support or information. For example, the developer must provide a 'general description of the weapon, its mission, and to conduct experiments on the weapons' effects'.[90] Although the U.S. Navy also assigns a single officer to each review, it imposes more stringent requirements that ensure that the review considers each of the IHL principles to ensure that the means and method of war under review is legal.[91] Both the Navy and the U.S. Air Force require that the review be conducted during the development process before acquisition. The Air Force requires that the assigned lawyer consider 'whether a specific rule of law prohibits or restricts the weapon's use, whether the weapon causes superfluous injury, and whether the weapon is indiscriminate in effect'.[92] Although they are split among the service branches and do not follow a centrally directed method, these review processes allow the United States to ensure that it does not violate treaties and customary law.[93]

Differences in How AUKUS Members Conduct Legal Reviews

A significant complicating factor in cross-comparison of the approaches of Australia, the UK and the United States to Article 36 legal reviews is the novelty of doing so. Such reviews have remained firmly under the control of individual states , which means that generating a

---

[86] Jared M. Cochrane, 'Conducting Article 36 Legal Reviews for Lethal Autonomous Weapons', *Journal of Science Policy and Governance*, Vol. 16, No. 1, 13 April 2020; DoD, *Review of Legality of Weapons Under International Law,* Department of Defense Instruction 5500.15, 16 October 1974.

[87] Boulanin and Verbruggen, 2017; DoD, *Implementation of, and Compliance with, Arms Control Agreements*, Department of Defense Directive 2060.01, 23 June 2020.

[88] DoD, 2023.

[89] Boulanin and Verbruggen, 2017.

[90] Ryan Poitras, 'Article 36 Weapons Reviews and Autonomous Weapons Systems: Supporting an International Review Standard', *American University International Law Review*, Vol. 34, 2018.

[91] Poitras, 2018.

[92] Poitras, 2018.

[93] Poitras, 2018.

common legal review process for autonomous systems would be a challenging endeavour. Comparing these approaches does, however, identify some aspects of the process that could be better aligned so that the review processes could become complementary even if they remain functionally stand alone. For example, each of process contains elements that can be found in the common features identified by Boulanin and Verbruggen, particularly compliance with established IHL principles and references to a check of existing treaty obligations.[94]

Unlike the UK and Australia, the United States is not formally bound by Article 36. Although its current processes appear to ensure compliance with IHL, they are grounded in policy and customary practice rather than in international legislative requirements. This difference in flexibility creates a risk that elements of future systems that violate IHL would block UK and Australian reviews but could be allowed under the U.S. process.

Additionally, each of these processes impose different approaches on the assigned reviewers and grant them different capacities to solicit information from the developer and from other elements of the military. This creates the potential for conflict over misaligned information requirements, barriers to cross-national information sharing, control of knowledge and challenges securing information from subject-matter experts in another state's military. Furthermore, unlike the UK and Australia, the U.S. system is single service–based rather than joint, which means that the U.S. contribution to a joint weapon review process would have to include individual service branch representatives or internally account for interservice differences in standards and processes. Finally, there are differences in the formality and power of the recommendations and results from such legal review processes. For example the UK process results in a formal written statement, and the Australian system has three potential outcomes, each of which is then formalised in the acquisition process. The U.S. system does not place the same formality or compliance restrictions on the result of its reviews.

However, there are commonalities between AUKUS partners that would make multinational or mutually recognised reviews possible. These commonalities include roughly comparable legal processes that stem from a common historical source of law (the UK common law system), similar commitments to ethically defensible military actions and an attendant reliance on social license as democratic state militaries, and the prevalence of common major defence firms and similar strategic doctrine for acquisition. In other words, general alignment across the AUKUS partners on the intent of legal reviews (if not on select aspects of the legal review process) and on the ethical principles suggests that legal and ethical factors will not be major deterrent to effective collaboration on military AI.

A more concerted effort to establish a shared approach to the implementation of responsible AI could provide the partners with a unique strategic advantage in terms of bolstering public support, expanding, and strengthening partnerships with other countries, and developing reliable systems that work as intended by human commanders and operators.

---

[94] Boulanin and Verbruggen, 2017.

There would certainly be value in developing and sharing public and multinational processes for conducting legal reviews of military applications of AI. In addition to the existing principles of IHL, AUKUS military lawyers could draw on emergent approaches for managing AI risk assessment and management, such as the National Institute of Standards and Technology's AI Risk Management Framework. Furthermore, it would be a valuable step to coordinate and harmonise the ethical military AI framework documents that each state has released. A multinational legal review process could be leveraged to demonstrate AUKUS commitment to shared ethical principles and IHL. This process could also allow for the inclusion external stakeholders and observers in the legal review process to better demonstrate that key ethical and legal principles are robustly incorporated into the design of future AUKUS military AI systems.

In the sections that follow, we explore some of the technical and regulatory challenges to collaboration that could pose a more significant barrier to the co-development of AI among AUKUS partners.

Technical Considerations

Testing and Evaluating Military AI

Test, evaluation, verification and validation (TEV&V) of new military systems is a necessary step for 'demonstrating a program's readiness for deployment',[95] that it will function reliably and expectedly.[96] However, the emergence of AI-enabled systems, particularly autonomous weapon systems, challenge traditional TEV&V mechanisms. The essential problem is that AI-based systems are complex, flexible and driven by stochastic processes. The often hidden interactions between elements in an autonomous system give rise to a far larger 'number of possible behaviours and the variety of "appropriate" ones'.[97] Unexpected or erroneous action by the system could be a result of a hardware fault, a data issue, misaligned sensor, malicious or inaccurate algorithms or just an emergent behaviour of a fully autonomous system.[98] The black box nature of current generation machine learning AI makes it difficult to determine the reason in real time, generating a complex web of potential actions that are difficult to translate into real-world replicable TEV&V processes. Existing TEV&V processes rely on an understanding of the causality between observed behaviour and known processes, which does not fit well with emergent learning systems. The nondeterministic nature of some AI-based systems means that TEV&V systems must

[95] Mario D. Williams and Phillyp C. Lawson, *Analyzing the Challenges and Obstacles to Developing and Fielding Autonomous and Semi-Autonomous Systems*, thesis, Naval Postgraduate School, 2020, p. 18.

[96] Maaike Verbruggen, 'No, Not That Verification: Challenges Posed by Testing, Evaluation, Validation and Verification of Artificial Intelligence in Weapon Systems', in Thomas Reinhold and Niklas Schörnig, eds., *Armament, Arms Control and Artificial Intelligence: The Janus-Faced Nature of Machine Learning in the Military Realm*, Springer, 2022.

[97] Heather M. Wojton, Daniel J. Porter and John W. Dennis, *Test and Evaluation of AI-Enabled and Autonomous Systems: A Literature Review*, Institute for Defense Analyses, 2020.

[98] Verbruggen, 2022.

somehow account for emergent behaviours, post-fielding learning and changes and the *convergence effect*, which occurs when integrating AI has unexpected effects at the system level.[99]

AI-based systems thus challenge traditional experimentation and evaluation models, and even the ranges within which those tests are performed. The potential for such systems to act in unexpected ways raises the risk to testers and bystanders. Complex systems tend to fail spectacularly and destructively, which is a serious concern when dealing with a self-targeting and potentially lethal system.[100] Nor do traditional ranges cater to the unique requirement of lethal autonomous systems: determining whether a correct target was correct, not just whether it was successfully engaged.

Security

The possibility of collaborating with partners on AI algorithms naturally raises cybersecurity concerns. In addition to the typical concerns focused on the security risks from humans, AI projects are especially vulnerable to security risks to their algorithms and stored data.[101] The most valuable component of an AI-based system, both in strategic terms and in pure resource investment, is the governing algorithm. Different partners might have different defensive cybersecurity capabilities and priorities, which potentially allow attackers to focus on the most vulnerable partner. Lastly, AI algorithms are vulnerable to *data poisoning attacks*, in which an attacker manipulates the data on which these algorithms are trained.[102] Our analysis suggests that expanding the number of data sources could allow adversaries to inject vulnerabilities into AI algorithms by identifying the least protected data set and exploiting it.

Export Control Regimes

The announcement of the AUKUS security pact attracted significant attention across the political and media spectrum for a variety of reasons, including that Australia would join the small number of states with whom the U.S. Navy has shared nuclear powered submarine technologies.[103] Yet the promise of increased technical research and development (R&D) cooperation towards shared military innovation has even more potential to affect future conflict.[104] The most significant hurdle to this cooperation for both the UK and Australia are stringent U.S. military export controls, the most difficult being the U.S. International Trade in

[99] Haugh, Sparrow and Tate, 2018; Verbruggen, 2022.

[100] Wyatt, 2021.

[101] Hoffman, *AI and the Future of Cyber Competition*, Center for Security and Emerging Technology, 2021.

[102] Hoffman, 2021.

[103] Abdul Rahman Yaacob, 'AUKUS Brings More Than Nuclear Submarines to Southeast Asia', East Asia Forum, 15 September 2023.

[104] Christianson, Monaghan, and Cooke, 2023.

Arms Regulations (ITAR), and information restrictions (particularly the extensive use of NOFORN).[105]

Existing Mechanisms for Co-Development and Intellectual Property Sharing

As befits a trio of closely allied countries with well over a hundred years of friendship and military cooperation, there are a variety of agreements and mechanisms for military R&D collaboration that well precede the AUKUS security pact. The Technical Cooperation Program, for example, was established in 1956 as a mechanism for Five Eyes states to collaborate on defence R&D. Guided by a representative Joint Executive Committee, the Technical Cooperation Program coordinates research across 11 focus areas, including electronic warfare and aerospace.[106] While the close intelligence linkages between the Five Eyes partners allows for sensitive information sharing, they have little scalability and would not be suitable for transitioning research into production.[107] It is more of a trusted network for sensitive research collaboration than a tool for multinational co-development or production.

As of the 2023 National Defense Authorization Act, all five countries are now considered part of the U.S. National Technology Industrial Base (NTIB), a mechanism that was originally established in 1992 to incorporate Canada into the U.S. military industrial base.[108] In 2017, the UK and Australia were added to the NTIB. [109] Although the expanded NTIB was meant to operate as a kind of Defence Free Trade Area that would enable 'seamless integration; of these states' military industrial bases, significant barriers remain.[110] For example, in the absence of costly political reforms, Australia and the UK remain barred from full access.[111] Recent research citing U.S. Congressional staffers suggests that it was adamant opposition from the U.S. State Department that 'using the NTIB as a way to even discuss export control reforms' was responsible for this distinct lack of progress.[112] It is noteworthy that this opposition occurred even though Australia and the UK are two of 28 countries with 'reciprocal Defence Procurement and Acquisition' MOUs with the United States and two of only 13 countries with security of supply arrangements.[113]

---

[105] NOFORN, or No Foreigners, is a security caveat from the U.S. system that restricts the document to cleared U.S. citizens; Demetri Sevastopulo, 'UK and Australia Urge Washington to Ease Secrecy Rules in Security Pact', *Financial Times*, 5 March 2023.

[106] Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt, *Forging an Alliance Innovation Base*, Center for a New American Security, 2020.

[107] The Five Eyes Agreement is an intelligence sharing arrangement encompassing Australia, Canada, New Zealand, the UK and the United States; Kliman et al., 2020.

[108] John G. McGinn and Michael T. Roche, *Developing a 'Build Allied' Approach to Increasing Industrial Base Capacity*, Naval Postgraduate School, 1 May 2023.

[109] McGinn and Roche, 2023.

[110] McGinn and Roche, 2023.

[111] Brendan Thomas-Noone, *Ebbing Opportunity: Australia and the US National Technology and Industrial Base*, United States Studies Centre at the University of Sydney, 2019.

[112] Greenwalt and Corben, 2023.

[113] McGinn and Roche, 2023.

This dissonance continues to influence the way that allies, who have been made wary by experiences with ITAR, view the U.S. government's commitment to genuine collaboration under Pillar Two. For example, the 2022 National Security Strategy explicitly called for removing 'barriers to deeper collaboration with allies and partners, to include issues related to joint capability development and production'.[114] The same year, the State Department released a statement that it does 'not anticipate any challenges in implementing AUKUS due to U.S. export control regulations', but that such regulations were important to 'safeguard U.S. technologies' and shouldn't be removed.[115] Recent efforts by U.S. lawmakers towards a legislative remedy that would exempt Australia and the UK from aspects of ITAR are a promising development and reflect a step towards resolving known issues from the perspective of both Australia and the UK.[116]

International Traffic in Arms Regulations

Established by the Arms Export Control Act of 1976, the ITAR are both the cornerstone of the U.S. framework for protecting its military technology and a lightning rod for those struggling to overcome collaboration barriers. At the heart of this dichotomy is the Cold War–era belief that U.S. allies represent a vulnerable backdoor that adversaries could leverage to undermine its technological advantage.[117] This concern was notably reinforced in the late 1990s, when the U.S. State Department revoked Canada's ITAR exemption and launched criminal prosecutions over a series of illegal diversions—or re-exports—of controlled dual-use technologies, including diversions to China.[118] To regain a reduced version of the exemption, Canada remodelled its export control laws by establishing the Controlled Goods Program in 2001.[119]

Australia and the UK have both developed defence export controls, but in neither case do they fully align with the United States. For example, although Australia requires export licenses for items on its Defence and Strategic Goods List, which are reviewed on a per-case basis, it does not impose the same level of end-use monitoring.[120] Nor is the moving of information within Australia subject to comparable scrutiny. In addition to enforcing its Strategic Export Control List, the UK estimates that it spends '$500 million annually on

---

[114] White House, *National Security Strategy*, 2022, p. 21.

[115] Greenwalt and Corben, 2023, p. 28.

[116] "More Work Needed on AUKUS Technology Sharing—British, Australian Officials', Reuters, 2 March 2023; Rachel Oswald, 'Lawmakers Seek to Ease Defense Export Controls to UK, Australia', 23 May 2023.

[117] Christianson, Monaghan and Cooke, 2023.

[118] Kristina Obecny, Gregory Sanders, Janes Ruedlinger and Jesse Ellman, *'U.S.–Canadian Defense Industrial Cooperation*', Center for Strategic and International Studies, June 2017.

[119] Government of Canada, *Key Events That Shaped the Controlled Goods Program*, last updated 5 November 2019.

[120] Lauren Sanders, 'AUKUS is supposed to allow for robust technology sharing. The US will need to Change Its Onerous Laws First', *The Conversation*, 13 July 2023.

ITAR compliance'.[121] These costs and the lengthy and complex approval processes contribute to the perception that U.S. restrictions harm its ability to marshal the resources of its allies to secure a technological advantage.

In addition to this 'outdated mindset',[122] problematic aspects of ITAR related to potential AUKUS co-development include its focus on knowledge and services rather than traditionally tangible military equipment,[123] the extraterritorial nature of the restrictions,[124] nonreciprocity, the burdensome compliance requirements, the imposition of further path-dependency, 'ITAR "taint"', and its failure to discriminate between allies and adversaries.[125] Chief among these 'deadly sins' are nondiscrimination, the risk of innovation becoming 'locked-in' to U.S. government direction, and the ITAR taint[126]. Unfortunately, ITAR does not offer effective provisions for close allies to gain exemptions or fast-tracked approvals for license requirements, with a limited exception for certain Canadian exports, effectively penalising states that prefer to collaborate with the United States rather than working with a variety of partners and providing a powerful disincentive for states to fully commit to the United States. Furthermore, because the U.S. process considers the whole of life export recipients, whereas Australia's does not, firms face the risk that they will lose control over the intellectual property in innovations that enter the U.S. system, further disincentivising them from selling to, or accepting funding from, the U.S. military.

Nonreciprocity of intellectual property is closely related to the most commonly referenced ITAR barrier, the *ITAR taint effect*, which refers to the fact that ITAR restrictions even attach to technologies or systems developed primarily by allies at the point at which U.S. knowledge is utilised and never go away.[127] This dynamic means that the developer must seek an ITAR license for any future exports or developments. As a result, the participation of any U.S. personnel, knowledge or equipment has significant consequences for a company's ability to secure export sales. Greenwalt found that many commercial innovators, even in the United States, viewed ;the prospect of an ITAR taint as an original-sin problem' that 'taints the product forever'.[128] Some firms (such as Anduril with its Ghostshark autonomous underwater vehicle program) even choose to work purely with commercial technology from the United States and only develop it into a military system in the host country using domestic researchers.[129] The effect of these restrictions is the generation of 'perverse incentives for U.S. companies to innovate abroad rather than at home',[130] which

---

[121] Bryant Harris, 'AUKUS Standoff: Australia, UK Wait on Congress to Approve Pact', *Defense News*, 5 September 2023.

[122] Greenwalt and Corben, 2023, p. 11.

[123] Kliman et al., 2020.

[124] Kliman et al., 2020.

[125] Greenwalt and Corben, 2023, p. 14.

[126] Greenwalt and Corben, 2023, p. 11.

[127] Greenwalt and Corben, 2023.

[128] Greenwalt, 2019, p. 13.

[129] Greenwalt and Corben, 2023.

[130] Christianson, Monaghan and Cooke, 2023, p. 8.

leads to ‘the U.S. military [closing] itself off from the global innovation market’ and undermining the purpose of Pillar Two of the AUKUS alliance.[131]

Meeting Distinct Operational Considerations

Among the potential friction points in co-design of autonomous systems is the different operational and strategic considerations that would underpin how such systems are deployed and the training of humans that continue to operate in their vicinity. Operational friction would likely result from the fact that an autonomous system would operate using training that it received from the developing entity; there would not necessarily be a mechanism for the importing state to make alterations.

The most direct comparison would be the lateral transfer of human personnel from foreign militaries, which has well-established precedent and policies in each of the AUKUS militaries. For example, the ADF’s Overseas Lateral Recruitment Scheme includes a selection board interview and places stringent restrictions on who can transfer, including a requirement of at least three years full-time service in the original military and the attainment of a Negative Vetting 1 level security clearance.[132] In 2014, a Defence official stated that approximately 30 junior officers and 35 senior noncommissioned officers were being recruited into the ADF per year through this program.[133] The U.S. and UK services have similar mechanisms. All such transfers would require some level of conversion training; examples vary from doctrinal familiarisation and equipment differences (for an infantry corporal for example) to qualification on another aircraft type. The need for such training is assessed on a case-by-case basis and delivered using traditional training pathways. If a human armour officer is transferred from the U.S. Army to the Australian Army, for example, they would have a comparable skillset, transferable Abrams tank experience and a similar doctrinal approach to commanding their crew. Where differences do exist (e.g. in relation to transitioning to the older M1A1 variant used by the Australian Army), they are relatively straightforward to identify and resolve during the transition or during predeployment exercises with the officer’s crew.

Identifying, understanding and rectifying these sorts of gaps or disconnects is far more complex in the case of autonomous systems and is arguably impossible without access to potentially sensitive training data. Even if we assume perfect reliability, an autonomous system could act in a manner that is unexpected by its human teammates because it was trained using data and methods derived from the developing military’s tactics, techniques and procedures. This potential challenge is particularly problematic in the case of decision support systems or AI-enabled commanders that are trained using data extracted from U.S. Army tactics and procedures but do not reflect the methods of British infantry or do not

---

[131] Greenwalt, 2019, p. 13.

[132] Defence Member and Family Support, *Overseas Lateral Recruitment: Defence Member and Family Support*, Australian Department of Defence, 2016.

[133] Seth Robson, ‘Job Pool Expanding for US Troops Interested in Heading Down Under’, *Stars and Stripes*, 1 April 2014.

incorporate data from foreign-designed systems. This kind of 'LT Siri' could, for example, suggest that an Australian infantry platoon commander take a particular path or assault a particular compound using a calculation that relied on assumptions (e.g. about air power or support weapon access) drawn from a U.S. unit.[134] Unexpected actions by autonomous systems (whether physical or not) increase risk to humans in the vicinity and damage the trust necessary for their effective use.

Although operational disconnect is a well-known challenge in coalition operations, the absence of a direct human operator places the onus entirely on the systems—and the processes around them—to overcome the resultant friction.

There are examples of a military successfully integrating a system into which it has limited insight into internal processes (e.g. the Aegis defence system and the use of pre-established intel mission data packages in the F-35).[135] In such cases, humans have remained on the decision loop and been able to develop familiarity with the system through experience. However, effective co-development of the system would allow each military to gain a detailed understanding of how that platform operates and makes decisions. Doing so would require that each AUKUS member be able to access and potentially modify the training data and core algorithms for the autonomous system. Such access could allow individual members to better understand the logic used by the AI and know which organisational adaptations would be required to incorporate it into their operational concepts.

Our analysis revealed three risks that might arise in the case of an importing state relying on a potentially inflexible non-human LAWS that was designed by another state, even when the values of both actors are broadly the same. The first risk is that the importer might have a different process for determining whether a target is legitimate. This situation was already seen during coalition operations in Iraq and Afghanistan, kill-capture missions and drone strikes, but also in relation to different militaries imposing varying restrictions on their owned air or artillery assets that affected when those assets were allowed to engage in support of allied forces. An autonomous system that is trained to another state's requirements might rely on particular behavioural patterns or insignia to identify whether a target is legitimate. If the importer has different rules of engagement, there is a risk that the autonomous system engages (or refuses to do so) unexpectedly.

Second, militaries have an obligation to their personnel to ensure that the actions of autonomous weapon system are sufficiently predictable and explainable. If they are not, then human commanders cannot legitimately be held responsible for an autonomous weapon's actions. For example, what if an autonomous system engages a target that its designer

[134] For comparison, a U.S. Army infantry platoon has 15 more personnel than an Australian counterpart and includes an integrated weapons squad (consisting of two Javelin anti-tank missile teams and two medium machine gun teams). Furthermore, a Australian Army platoon has significantly less organic access to specialised firepower and instead relies on detachments from the battalion Direct Fire Support Weapon Platoon.

[135] Our thanks to Carl Rhodes for raising this example.

considered legitimate but the deploying state did not?[136] If the human commander could not reasonably foresee this risk, then how can they legitimately be held legally responsible?

Finally, policy decisions must remain predicated on the recognition that autonomous weapon systems will not replace humans in combat entirely. Therefore, states have an ethical obligation to ensure that the autonomous weapon system, when operating within expectations, does not take actions that violate the conscience of friendly personnel operating alongside it. For example, if an autonomous weapon system were to engage a sniper in a residential building with an explosive round, it could kill civilians. In addition to the legal question, the human soldiers would have to live with the psychological cost of its aftermath, placing them at a greater risk of moral injury.

Although each of these risks are present in single-country development efforts, they are particularly problematic in the case of co-development or importation of autonomous weapon systems because the developer would be exporting its values and interpretations of international norms, as well as the physical system. In this case, we can draw a less noble comparison with special forces collaboration in Iraq and Afghanistan. An insidious culture was able to spread that encouraged violence against civilians in multiple national contingents.[137] Among the benefits of autonomous systems is that, so long as they are correctly designed, they are immune to the psychological strain that allowed this culture to spread and will retain the same embedded values despite multiple deployments.[138]

It appears, therefore, that different operational requirements or intended roles among AUKUS partners would increase the risk that a co-design process might lead to a suboptimal system that only meets a portion of the criteria for each actor. One avenue for cross-national friction would be disconnect in the intended use case for a given autonomous system, which would in turn affect the capabilities of that system. For example, consider how each state is experimenting with autonomous unmanned surface vessels. The U.S. Navy has invested in the Sea Hunter program, among other avenues, which demonstrates its interest in developing a capability that can contribute to a high-tempo great-power conflict and its desire for long-range deployable capability.[139] By contrast, the Royal Australian Navy (RAN) is experimenting with automating decommissioned offshore patrol vessels, [140] which reflects its desire to use the technology as a supplemental surveillance and security asset. This disconnect is reflective of the fact that the U.S. Navy and RAN have different operational environments, mission responsibilities and resources. This example also demonstrates the risk that a collaborative development process either delivers an overdeveloped and expensive

---

[136] Returning to the human example: Any lateral transfer would be required to understand, and expected to follow, the rules of engagement of their new military, not their original one.

[137] Matthew Cole, *Code Over Country: The Tragedy and Corruption of SEAL Team Six*, Public Affairs, 2022; Shannon Torrens, *War Crimes in Afghanistan: The Brereton Report and the Office of the Special Investigator*, Parliament of Australia, undated.

[138] Austin Wyatt, *The Disruptive Impact of Lethal Autonomous Weapons Systems Diffusion: Modern Melians and the Dawn of Robotic Warriors*, Routledge, 2021.

[139] Wyatt, 2021.

[140] 'Austal to Undertake Patrol Boat Autonomy Trial for RAN', Australian Defence Magazine, 7 October 2022.

capability to the junior partner or results in a capability that is just good enough for each participant and fails to deliver on the disruptive promise of this technology.

Although the tension around trade-offs in military co-development has been documented in prior cases, we argue that it is exacerbated in the case of autonomous weapon systems because of their reliance on pre-established training data.[141] The capability to operate in different operational environments or roles would largely be dependent on being able to develop separate modules or variants in the training datasets. The initial costs involved in creating and maintaining these data sets naturally skews the resultant systems towards the requirements of the largest contributor, as well as a level of path dependency on subsequent systems. One potential mitigation avenue would be for Australia to focus on the creation or modification of a training dataset relevant to operations and environments that are of more direct interest to the ADF.

Finally, although autonomous systems are not reliant on specific controlled materials or difficult to attain knowledge (key non-proliferation levers for nuclear weapons) to the same degree as conventional weapons, there are still potential chokepoints and supply-chain risks associated with advanced AI—particularly around semiconductors, and high-capacity compute. The conventional approach would be to mitigate this risk by onshoring (or ally-shoring) a level of production capability. However, as demonstrated by the U.S. experience with the CHIPS and Science Act of 2022, onshoring semiconductor production requires significant infrastructure investments that would likely be beyond the capacity of Australia.

[141] Marc R. DeVore, 'International Armaments Collaboration and the Limits of Reform', *Defence and Peace Economics*, Vol. 25, No. 4, August 2014.

Chapter 4. Resource and Cooperation Considerations for Junior and Senior Partners

It is worth stating explicitly that multinational co-development of defence technologies largely occurs because partners 'lack the necessary financial resources or expertise to achieve their capability goals' and 'hope that together . . . they will have enough resources and expertise to develop the desired capabilities'.[142] But the economic dimensions of collaboration—especially in advanced technologies for which the commercial sector also has a significant role in development—are complex and potentially barrier-inducing. Advanced capabilities can have significant associated costs, requiring high levels of investment, resourcing and expertise.[143] Because of what has been termed the 'arithmetic of defence policy', countries are increasingly moving towards multilateral configurations similar to AUKUS.[144]

Indeed, costs might ultimately extend beyond the economic context to, for example, dependency on partner supply chains, toleration of delays as a result of onerous coordination requirements and, significantly, surrender of some level of national autonomy.[145] These are of particular importance under an such agreement as AUKUS because junior and senior partner dynamics, whether for Pillar One or Pillar Two, inform the parameters of the agreement. The agreement is built on existing collaborative architectures, such as NTIB, which have known obstructions and inadequacies because they 'posit allies as junior partners with limited value-add to matters of defence industry and technology collaboration'.[146] If this is not sufficiently addressed, it can have significant implications for the extent to which AUKUS fosters interoperability and harmony across the complex processes and requirements that, Nemeth argues, are factors that 'must be positioned at the forefront of multinational capability development programs from the beginning'.[147]

Each party has a unique strategic intent regarding the agreement and affords weight to different sovereign dimensions. Hence, there must be clarity on alliance management and dynamics and whether AUKUS is best used, as one commentator has expressed, 'as a battering ram or a surgical scalpel'.[148] Here, the particular model of capability development could be important. Nemeth outlines the following four models:

---

[142] Bence Nemeth, 'Military Innovation and Capability Development in a Multinational Context: The Costs and Benefits of Multinational Cooperation', *Air Power Journal*, Fall 2022, p. 7.

[143] Nemeth, 2022, pp. 2–3.

[144] Michael Alexander, and Timothy Garden, 'The Arithmetic of Defence Policy', *International Affairs*, Vol. 77, No. 3, July 2001.

[145] Nemeth, 2022, p. 7.

[146] Greenwalt and Corben, 2023, p. 24.

[147] Nemeth, 2022, p. 10.

[148] Corben, 2022.

- Pooling of capabilities. Capabilities remain nationally owned but are integrated into a collective structure.
- Sharing of capabilities. Select capabilities are made available in the multinational context, but control is retained by nation, and forces are not integrated.
- Role- and task-sharing. Support is provided to each partner to plug capability where capabilities are not necessarily owned.
- Pooling through acquisition. This model consists of two parts: (1) combined acquisition, in which a capability is procured, maintained and operated jointly; there is no national control; and the capability is used by way of set arrangements; and (2) co-development, in which nations jointly develop and produce a capability.[149]

Of principal importance in delivering capabilities, across any of the models, is clarity from each party about what they can provide and areas in which there might be significant constraints. Moreover, there needs to be upfront acknowledgment that each AUKUS partner will 'have differing commercial equities at play and the desire to maintain and build their areas of comparative advantage and market share'.[150] This competitive dimension should not be seen as a negative. Market competition drives innovation; the challenge is to harness and maximise the different approaches.[151]

One way to identify and integrate these constraints—along with the unique perspectives of Australia, the UK and any future partners—would be to embed end-user based combined red-teams in the design and development stages of high-risk systems (e.g. systems intended to operate in high-risk environments or deploy lethal payloads). Doing so would help identify risks and opportunities from alternative perspectives.

Although the agreement is outwardly one of compatibility and shared interest for the junior partners in AUKUS, there might be veiled risks, particularly in terms of discretionary decisionmaking and operational autonomy. For technological collaboration within AUKUS to work, the value and worth of allied inputs must be understood in terms of collective efforts.[152] Without this, key stakeholders could be disincentivised to work within AUKUS parameters for fear of losing control over intellectual property or overcommitting resources and human capital to comply with regimes that are too cumbersome.[153] Cognisance of the contributions and investments required of the respective parties is key.

Australia possesses substantial equities on which to capitalise (e.g., human capital, research institutions, quantum physics, its capacity for raw materials), which make it an important contributor to partner supply chains. There also continues to be relatively low levels of commercialisation, integration of government, industry and academia is still lacking, and levels of R&D funding and science, technology, engineering, and math skills need to be increased,[154] which will have knock on effects for AUKUS collaborations.

---

[149] Nemeth, 2022, pp. 5–7.

[150] Jackett, 2022, p. 20.

[151] Jackett, 2022.

[152] Greenwalt and Corben, 2023, p. 10.

[153] Greenwalt and Corben, 2023, p. 10.

[154] Jackett, 2022., p. 24.

Therefore, the level of investment Australia has made in terms of funding and resources across both Pillar One and Pillar Two workstreams is substantial, to the extent that the observation has been made that, in Australia, 'AUKUS has virtually restructured the entirety of their defence and foreign affairs thinking'.[155] Accordingly, there are important questions to ask about what junior partner sovereignty looks like within AUKUS if the expectation, both domestically and in the United States, is a fundamental restructuring of various parts of defence supply chains and defence innovation networks and systems to further alliance interests. Certainly, this is what is occurring in Australia.

As discussed previously, onerous U.S. bureaucratic mechanisms, particularly ITAR and foreign military sales compliance measures, could cause operational autonomy issues for the other members. Christianson, Monahan and Cook notes that the UK 'spends at least half a billion dollars per year complying with the [ITAR]—or nearly 1 per cent of its defence budget'.[156] The processes entailed within could have the potential to impede allied deployment of forces. An example of this occurred when a routine sonar upgrade on British Royal Navy submarines suffered significant delays because of foreign military sales compliance. The ITAR regime meant that 'a separate submarine could not dock at sea for maintenance until the Department of State approved an ITAR-controlled component'.[157] There have been some efforts to 'smooth the regulatory runway' for multinational defence cooperation.[158] However, for bureaucratic impediments, in the case of AI as an example, such barriers could lead to not only integration and development issues but also system failure.[159]

Barriers relating to the development of emerging technologies, particularly in the military space, can vary from those of a technical nature; associated supports; appropriate resourcing, (which can be an impediment even in those countries that can rely on advanced technical and industrial capabilities but also span organisational challenges); complexities around acquisition and procurement; legal and ethical considerations; experimentation and testing and evaluation issues and cultural acceptance.[88]

The perennial valley of death concern,[160] although it generally refers to innovation in the commercial sector, also applies to defence actors. Indeed, their natural reliance on a single key customer (for example, the Australian military) means that defence sector firms are particularly vulnerable to delays in the selection and acquisition process. This is particularly problematic in the case of low-technology readiness levels technologies or those technologies for which the commercial sector absorbs the majority of available talent, such as AI-related technologies. Delays or uncertainties in funding disincentivise investment in risky defence start-ups and encourage prime firms to invest in proven platforms. Although emerging

---

[155] As quoted in Jennifer D. P. Moroney and Alan Tidwell, 'Making AUKUS Work', *RAND Blog*, 22 March 2022.

[156] Christianson, Monaghan and Cooke, 2023.

[157] Christianson, Monaghan and Cooke, 2023.

[158] Oswald, 2023.

[159] Christianson, Monaghan and Cooke, 2023.

[160] The *valley of death* refers to the point at which a technology becomes stranded in the space between an initial technological discovery and its adaptation into a product or capability.

technologies might be able to reduce this impact by relying on dual-use capability, militaries cannot rely solely on doing so to incentivise rapid development. In recognition of this challenge, AUKUS members have made significant efforts to circumvent onerous development and acquisition processes through the development of innovation hubs, which facilitate engagements across military, industry, academia and the entrepreneurial community.[161] However, significant barriers remain, and in some cases could become entrenched by AUKUS dynamics.

For example, in the case in which challenges associated with guiding a technology from discovery to impact come from underperformance in knowledge, skills, technology outputs and poor research translation, there might be inadequate investments in riskier emerging technologies. Although the associated commercial or investment challenge might be met by the movement of innovations to larger markets, such as the United States, where they might be readily monetised, this movement could also result in an inability among junior AUKUS partners, to pursue, in relative terms, indigenous innovation to the same extent as their counterparts.[162]

[161] Examples of these hubs include the U.S. Defence Innovation Unit (DIU) and Joint Artificial Intelligence Center (JAIC), the UK's jHub program and Australia's ASCA.

[162] Jackett, 2022, p. 13.

Chapter 5. Gathering Insights on Military Technology Collaboration

Having established an understanding of key challenges and opportunities for military technology collaboration between allies from our analysis of the literature, it is important to present evidence from prior attempts to co-develop military technologies and to understand the perspectives of experts that are actively working on related issues.

Concerns Raised by Policymakers and Artificial-Intelligence Experts

To understand the concerns around and potential inhibitors to the co-development of AI between the United States and its allies and partners, we sought input from experts from of close allies and partners of the United States. We interviewed thirteen experts in AI and defence policy from five different U.S. allies and partners. Some of our interviewees work for their national governments; others are policy experts at think tanks in these nations. Each of the individuals has a background in either AI or defence cooperation. These experts were identified through a review of public documents and our professional knowledge of the field within the Asia Pacific. Interviewees were guaranteed anonymity as a condition of participation to enable them to provide candid responses on a politically sensitive topic. The insights presented in this section are derived from those interviews.

Conceptual Problems

Interviewees noted that some of the primary potential blockers to the co-development of AI with the United States are conceptual. Although allied policymakers often discuss AI as a potential gamechanger, most of these policymakers do not have a specific use case on which they are focused. Conversations about the potential joint development of AI too often remain vague. Interviewees noted the need to converge on the purpose of AI co-development. As one interviewee stated, ‘AI in order to do what exactly?’ These concerns speak to the relative lack of technical expertise among some policymakers and the lack of clear priorities for AI development. While these concerns would also hamper the independent development of AI by U.S. allies, co-development of AI requires concrete projects that use AI.

Additionally, our interviewees indicated that they do not perceive a clear understanding on the part of our American allies and partners as to what the co-development of AI would mean in practice. Interviewees hypothesised several different interpretations of the co-development of AI. In its simplest form, the co-development of AI could mean that the United States develops AI algorithms and then provides the resulting model to allies for use in their own military applications. At a more robust level, the co-development of AI could involve data-sharing agreements between the various partners while the actual AI models are developed and trained independently. At the most robust level, the various participants in the co-development project would collaborate on the research and engineering tasks required to

train AI models and develop AI applications using those models. Our interviewees expressed that they were unclear which form or forms the co-development of AI would ultimately take.

Infrastructure and Data

Another frequently cited issue was the lack of foundational infrastructure to develop AI models and potential issues around aligning data standards between the United States and its collaborators. On the infrastructure side, even better-funded U.S. allies do not have the same order of magnitude of resources available to purchase compute and storage capacity or operate data centres at the scale of the U.S. military. Although the prospect of sharing common infrastructure is attractive to U.S. allies, larger allies could have concerns about the perception of the loss of sovereignty (and the loss of pride) if they are perceived as becoming dependent on a capacity they do not own. A loss of sovereignty in these technologies raises the risk that a state could lose its freedom to develop, maintain and modify the resulting systems. Allies might also have some concerns about lock-in on infrastructure provided by the United States: If the shared infrastructure diverges too much from widely available commercial alternatives, it could result in some hesitation on the part of allies to become dependent on a capability they cannot easily replicate.

Interviewees also frequently cited potential blocking issues involving data-sharing and data interoperability. These concerns took different forms. Many interviewees discussed regulatory barriers for data that contain personally identifiable information, such as the Government Data Protection Regulation (GDPR) or other domestic regulations. Interviewees often mentioned policy barriers even for military data that did not contain any personally identifiable information and was unclassified. Data sharing often requires a memorandum of understanding (MOU) that cannot be easily reused for different organizations or for different purposes; one interviewee described a time when they needed to leverage five different MOUs in parallel to allow their engineering team access to data needed for a military AI project. In theory, many bureaucratic steps could be removed for less sensitive military data (i.e. data from outside the intelligence branch). However, in practice, many organizations are hesitant to share any kind of data because of risk aversion and institutional protectionism.

Finally, one interviewee noted their nation's concern that any algorithms developed cooperatively might not be compatible with other software applications and systems used by its military. For example, because this nation is not primarily an English-speaking nation, there are concerns that software products primarily developed by American companies will not be fully compatible with this nation's language or with the processes and procedures of its military. While careful engineering of software applications can address these concerns, worries about the compatibility of systems persist.

Intellectual Property Concerns

Concerns about intellectual property rights were often top-of-mind for our interviewees. Our interviewees recognised that any co-development of AI would intimately involve defence contractors and technology companies. Several interviewees expressed concerns that allies and partners would not receive the same treatment from corporations as their American

partners would. As one interviewee noted, ‘we have questions about how much the U.S. will actually share with us and whether the U.S. would actually allow us to be fully involved’. Respondents also recognised that companies would want to protect any AI models that they created and would not want to share their intellectual property with others.

Two of our interviewees specifically cited concerns around ITAR; one of these interviewees described it as a potentially ‘huge problem’. One interviewee expressed the concern that ITAR could prevent a country from getting its own data back after it had been shared and wondered how ITAR would be interpreted for an AI model that had been trained on data from many partners. They also worried that ITAR could be applied after the fact to a collaboratively developed AI application. They noted that agreements between the partners or other up-front reassurances could help prevent these concerns from inhibiting collaboration.

Case Studies in Military Technology Collaboration

Although AI is an emerging disruptive technology, militaries attempting to pool their resources to develop new platforms is not new. The incentives and challenges that affected prior attempts at multinational co-development, even among strong allies with closely linked industrial bases, are therefore worth highlighting. The following section primarily considers two case studies: the Future Combat Air System (FCAS) and the Nulka Active Missile Decoy. We chose these case studies because they offer insights into distinct components of the challenge of AI collaboration within AUKUS. The FCAS is an ongoing high-technology development effort that is led by three states with close industrial links, similar doctrines and a broadly successful track record of similar co-development efforts. The Nulka Active Missile Decoy, on the other hand, is a well-documented example of a successful effort: The Australian technology was developed in partnership with the U.S. military industrial base and transitioned into an effective military capability that remains in deployment. Both cases illustrate the value of common conceptual approaches, the challenges of domestic and industrial pressures, and the impact of regulatory and technical barriers.

Future Combat Air System

When considering the challenges posed by co-development of advanced conventional weapon systems, the European experience is illustrative. There is a long history of co-developing such systems (including the Eurofighter Typhoon),[163] and establishing initiatives for combined funding of such projects (including the European Defence Fund’s Permanent Structured Cooperation program).[164] The FCAS is the latest in these efforts. The FCAS is a combined development project between Germany, France, and Spain that began in 2020 to develop a system of systems built around a sixth-generation fighter aircraft.[165] Aside from the future fighter aircraft, the core known components of the system are a combat cloud and an

[163] Nemeth, 2022.

[164] Nemeth, 2022.

[165] Justin Bronk, ‘FCAS: Is the Franco-German-Spanish Combat Air Programme Really in Trouble?’ Royal United Services Institute, 1 March 2021.

unmanned combat aerial vehicle (UCAV) collaborative combat aircraft.[166] This case study offers valuable insights into the challenges involved in co-developing a system even when the members of the project have a successful collaborative history.

However, it is important to note that there are significant differences between this case study and the core question of this report. The FCAS coalition has a far less sophisticated intelligence sharing regime than AUKUS and is not militarily allied in the same manner. Nor do the two cases have the same goals. The FCAS project is designed to deliver an air dominance system of systems—a discrete package—whereas AI co-development under AUKUS Pillar Two is a broader enabling technology with a wide variety of potential use cases. Although this obviously distinguishes the two scenarios, the divergence aids in this analysis because FCAS is a less ambitious arrangement that builds on a well-established glide path towards a distinct platform.[167] If a challenge cannot be resolved, it would likely be of more significant impact in an attempt to co-develop an AI-enabled system under AUKUS arrangements.

However, there are similarities between FCAS and AUKUS. For example, in both cases there is a clearly junior partner, at least from a financial and industry perspective. In FCAS, that partner it is Spain; in AUKUS, that partner is Australia. Spain's 2022 defence budget ($20.3 billion USD) was dwarfed by Germany ($55.8 billion) and France ($53.6 billion).[168] Spain was ranked the ninth-largest arms exporting state in 2021;[169] just one firm was among the top 100 (Navantia, a shipbuilder).[170] By comparison, France was the third-largest arms exporter in the world,[171] and Germany was the fifth-largest exporter.[172] France had five firms and Germany had four firms in the top 100.[173] Although the United States dominates the AUKUS partnership in terms of military expenditure ($877 billion USD) and its share of global arms exports (39 per cent),[174] the UK is globally competitive in both budget ($68.5 billion USD) and export share (seventh in the world at 2.6 per cent).[175] Australia is clearly the

[166] Bronk, 2021.

[167] Nemeth, 2022.

[168] Dominic Vogel, *Future Combat Air System: Too Big to Fail; Differing Perceptions and High Complexity Jeopardise Success of Strategic Armament Project*, German Institute for International and Security Affairs, 2021.

[169] Pieter D. Wezeman, Alexandra Kuimova and Siemon T. Wezeman, 'Trends in International Arms Transfers, 2021', fact sheet, Stockholm International Peace Research Institute, 2022.

[170] Lucie Béraud-Sudreau, Xiao Liang, Diego Lopes da Silva, Nan Tian, and Lorenzo Scarazzato, 'The SIPRI Top 100 Arms-Producing and Military Services Companies, 2021', Stockholm International Peace Research Institute, December 2022.

[171] Wezeman, Kuimova and Wezeman, 2022.

[172] Wezeman, Kuimova and Wezeman, 2022.

[173] Béraud-Sudreau et al., 2022.

[174] Tian et al., 2023; Wezeman, Kuimova and Wezeman, 2022.

[175] Tian et al., 2023; Wezeman, Kuimova and Wezeman, 2022.

junior financial partner; it spent $36 billion on defence in 2022 and secured only 0.6 per cent of global arms exports.[176]

Furthermore, Spain's integration into the FCAS project is viewed as a test case for future entrants,[177] particularly if the British-Italian-Japanese Tempest program was to be merged in the future.[178] Potential expansion has been a repeated source of speculation since AUKUS was first announced; even UK House of Commons Foreign Affairs Committee recommended that the UK push for Japan and South Korea to be invited into AUKUS. [179] The potential future expansion of AUKUS relates closely to concerns raised by some of our interviewees.

In their analysis, both Vogel and Bronk identify three challenges around the FCAS co-development process.[180] These challenges are particularly applicable to an AUKUS AI co-development project and are thus of particular importance to our analysis.

The first challenge is that, in both cases, there are differences in the types of power projection in which contributors engage and in their view of their role in the world order. In FCAS, for example, France has territory to protect in the Asia Pacific and has previously leveraged air and ground power to intervene in North and Sub-Saharan Africa; Germany was derided repeatedly by the media and the U.S. government before the 2022 Russian invasion of Ukraine for an overly pacifist and inward-looking approach to European security.[181] Similarly the United States has global security interests and responsibilities as the incumbent hegemon, which necessitates the ability to globally project hard power. The UK has also recognised the need for robust power projection capability to directly influence the Asia Pacific.[182] In contrast, the 2023 Defence Strategic Review firmly reinforced a regional view of security in Australia; the ADF focuses on capabilities to deter a great power aggressor in its immediate vicinity, such as long-range maritime fires and asymmetric operation capability.[183]

In both FCAS and AUKUS, these conceptual differences affect how the members view the technology, invest their resources and prioritise design factors. This dynamic touches on similar conceptual concerns as those identified in the interviews. Beginning with FCAS, consider how differences in intended operational purpose and requirements for the aircraft

---

[176] Julian Kerr and Andrew MacDonald, 'Australia's 2022–23 Defence Budget Climbs by 7.4%', *Janes Defence News*, 30 March 2022; Wezeman, Kuimova and Wezeman, 2022.

[177] Dominic Vogel, , *Future Combat Air System: Too Big To Fail; Differing Perceptions and High Complexity Jeopardise Success of Strategic Armament Project*, German Institute for International and Security Affairs, 2021.

[178] The Tempest program (also known as the Global Combat Air Program) is a British-Italian-Japanese collaboration on a sixth-generation fighter program that is similar to the FCAS; Bronk, 2021.

[179] Foreign Affairs Committee, *Tilting Horizons: The Integrated Review and the Indo-Pacific*, Eighth Report of Session 2022–23, UK Parliament, 20 August 2023.

[180] Bronk, 2021; Vogel, 2021.

[181] Bronk, 2021.

[182] Foreign Affairs Committee, 2023.

[183] Australian Department of Defence, *National Defence: Defence Strategic Review*, 2023.

according to each developing state, in this case four services across three states.[184] France, for example, require the capacity to operate from their aircraft carrier; Germany is primarily interested in an air-superiority capability.[185]

In the case of AUKUS, although each state is attempting to deter aggression by the same actor in the same region, different strategic requirements affect investment decisions. Take, for example, co-development of an autonomous UCAV. Although the United States and UK would likely prioritise carrier-based capability and the ability to survive inside an adversary's ground-based air defence umbrella; Australia would be more likely to prioritise maritime strikes and air-to-air refuelling.

This complexity also interacts with the second relevant challenge: the ethical and domestic political differences that complicate key design features, in this case over whether the future fighter should have nuclear capability and whether the supporting UCAVs (known as remote carriers in FCAS) should be armed. For France the future fighter needs to be able to deliver the aerial component of their nuclear deterrent; it must be able to do so from their aircraft carrier, and France has demonstrated a willingness to deploy armed UAVs.[186] Although Germany does have access to nuclear weapons through NATO sharing arrangements (and some U.S. gravity bombs are stationed in Germany), the capability is subject to far greater domestic political controversy. Therefore, it is unlikely that the German government would push nuclear armament capability as a significant design factor in a future air fighter.[187] Similarly, in the case of arming UAVs, there was far more significant public resistance and debate around the ethics of such systems when the German government mooted their acquisition, finally acquiring missiles for their Heron UAVs in 2022.[188] Spain sits somewhere in the middle. It has no nuclear deterrent requirement and does not have access to NATO nuclear sharing arrangements. Spain has purchased armed Reaper UAVs from the United States and is a participant in the nUEROn UCAV program, but the Spanish parliament has not explicitly debated a legal position on LAWS.[189]

Finally, there are the well-known challenges associated of balancing capability with each participant's natural inclination to maximise the level of effort for domestic industry. In the FCAS program, the participants adopted a 'best athlete' principle that divides seven pillars of effort among the participants using knowledge of their proven capabilities.[190] Under this model German firms lead the UCAV and combat cloud pillars, France leads the aircraft and engine pillars, Spain leads the sensor and stealth pillars (although the head contractor on the

---

[184] Amos Dossi and Niklas Masuhr, 'European Fighter Programs: A Preliminary Assessment', *CSS Analyses in Security Policy*, Vol. 291, October 2021.

[185] Bronk, 2021.

[186] Vogel, 2021.

[187] Vogel, 2021.

[188] European Forum on Armed Drones, 'Germany', webpage, undated-a; 'Germany to Get Weaponized Drones for the First Time', *Defense Post*, 6 April 2022.

[189] European Forum on Armed Drones, 'Spain', webpage, undated-b.

[190] Vogel, 2021.

latter is Airbus) and simulation is shared.[191] The program is further complicated by the difference in how each state government interacts with its defence industry. Germany and Spain have moved towards a pan-European vision of strategic autonomy, and the French government is far more deeply integrated with its defence industry and explicitly pursues the promotion of French sovereign capability.[192]

Nulka Active Missile Decoy

Although the AUKUS members do not have the same track record of co-developing major platforms as the European states, technology and intelligence-sharing is a well-established strength of the U.S.-UK-Australia relationship. Thus, far from a standing start, collaboration in AI technological development can build on a long-standing tradition of military technology and research collaboration between each of the member states. There is less experience, however, in how to convert collaborative research into true co-development of military platforms. The Nulka Active Missile Decoy was chosen as a case study because it is the most successful example of an Australian-U.S. co-developed capability.

The Nulka Active Missile Decoy is essentially a hovering rocket launched from an off-board system.[193] The Nulka contains an electronic warfare payload that is designed to fool sea-skimming antiship missiles.[194] It is currently deployed on more than 150 vessels across the Canadian, U.S. and Australian Navies.[195]

Beginning as a technical concept within the Australian Defence Science and Technology Group (DSTG), the Nulka was successfully matured and brought into service in response to a strategic shock.[196] Its pathway demonstrated the value of high-level leadership engagement, the importance of working-level connections and the impact of disruptive strategic shock on barriers to collaboration. These lessons can be applied to the development of military applications of AI.

The original concept of the Nulka was conceived by an Australian defence scientist in the early 1970s; DSTG began engineering development in early 1975. A major early decision point was to focus on developing a variable-thrust, solid-propellant rocket motor instead of a rotary-blade design.[197] Initial demonstrator testing was completed by 1981, and DSTG sent several delegations to the United States to secure a development partnership over the

---

[191] Vogel, 2021.

[192] Vogel, 2021.

[193] Defence Science and Technology Group, 'Nulka Active Missile Decoy', webpage, 2023.

[194] Marcus Hellyer, *Cracking the Missile Matrix: The Case for Australian Guided Weapons Production*, Australian Strategic Policy Institute, 2021.

[195] BAE Systems, 'Nulka Active Missile Decoy', webpage, undated.

[196] DSTG is the current name for Australia's primary defence science agency. As part of the Australian Government's response to the 2014 First Principles Review, the organization was renamed from the Defence Science and Technology Organisation. While these events largely occurred before the name change, for the sake of consistency, this report uses the organisation's current name.

[197] David Gambling, Mal Crozier and Don Northam, *Nulka: A Compelling Story: Ingenuity, Partnership, Perseverance*, Australian Department of Defence, 2013.

following years. However, 'no substantive discussions on specifications, advanced development programs and timings' occurred until 1984.[198]

During this period, the need for such a system was dramatically illustrated by the development and deployment of the French Exocet missile, a sea-skimmer that flew below radar and existing hard-kill countermeasures. The sinking of the UK's HMS *Sheffield* in 1982 was a significant strategic shock that galvanised efforts to find some sort of response.[199] Despite the *Sheffield* incident, strong institutional resistance to the Nulka continued until a shift in strategic priorities towards smaller vessels occurred as a result of the scrapping of plans for a future RAN aircraft carrier and the U.S. Navy's experiences in the Iran-Iraq war.[200] These changes, along with the early diffusion of sea-skimmer technologies and the strike on the USS *Stark* in 1987,[201] made the value of the Nulka decoy clearer.[202] This aspect of the Nulka's history highlights the interaction between institutional resistance to emergent disruptive technologies and the impact of strategic shock. We also saw this in early U.S. engagement with the Predator drone, and expect to see similar influences on the development of LAWS.[203]

The next stage in the Nulka's development was later described in the DSTG-commissioned program history as 'characterized by detailed negotiations between the United States and Australia in an attempt to reach consensus on technical requirements and funding prior to a formal agreement being signed by the parties'.[204] This phase is notable for our purposes because these negotiations had stalled until a meeting between Kim Beezley (the Australian Minister for Defence) and Caspar Weinberger (the U.S. Secretary of Defense) in 1985. The DSTG history records Beezley's recollection of the events:

> I had papers on the Winnin project with me when I met Cap Weinberger by accident, prior to joint defence meetings. Winnin was not on the agenda. I had the papers because the Department had concluded that the American interest in the Australian decoy was waning and it appeared as if the Winnin project would have to be terminated. Weinberger's response to me was along the lines of 'I am sick of you always complaining about this. You say you want us to buy but you never present me with practical proposals'. The light bulb went on and I reached back into my briefcase for the Winnin papers and replied 'what about this?' We then had a brief discussion about the project and Weinberger instructed his officials to ensure the success of the project—no matter what![205]

---

[198] Gambling, Crozier and Northam, 2013, p. 57.

[199] DSTG, 'How the Falklands War gave rise to Australia's Prize Defence Export—After Years of Struggling with Reluctance', 6 May 2022.

[200] Gambling, Crozier and Northam, 2013.

[201] DSTG, 2022.

[202] Gambling, Crozier and Northam, 2013.

[203] Richard Whittle, *Predator: The Secret Origins of the Drone Revolution*, Macmillan, 2014.

[204] Gambling, Crozier and Northam, 2013.

[205] The Winnin Project was the original name for the Nulka development program; Gambling, Crozier and Northam, 2013.

Although this is Beezley's recollection and the details cannot be independently verified, it is illustrative of the importance of high-level leadership engagement, particularly in the case of multinational projects. The importance of senior leadership engagement and support for the success of military innovation is well documented.[206] For example, in 2023, the Congressional Research Service identified it as a key barrier to Directed Energy Weapons development in the U.S. military.[207]

These negotiations culminated in a full-scale collaborative engineering development MOU on 10 August 1986.[208] Under the agreement that there was a commitment by both states to share all intellectual property and to allow firms from either state to compete for work whether production was combined or not.[209] Early progress on the Australian side was complicated by the coincidental release of the Dibb review the same year.[210] The overall division of labour placed responsibility for developing the payload on the U.S. side, led by Lockheed Martin Sippican, and the development of the platform on the Australian side. The Australian prime was AWA Defence Industries, although significant personnel time was allocated from the DSTG to support engineering development.

Although signing an MOU agreeing to share intellectual property and collaboratively develop the technology appears to successfully combat of some of the issues identified previously, such as nonreciprocity and ITAR taint, it was not the case in practice. The Nulka decoy was, as its name makes clear, an Australian technology.[211] The post-MOU development and engineering was focused on maturing the delivery system and electronic warfare component. The U.S. components were handled by an U.S. company with a clear distinction drawn between the two teams.[212] Unfortunately the result was that the final product suffered from 'ITAR taint' and is now subject to ITAR restrictions despite originating as an Australian technology. This was most clearly demonstrated in 2007, when Lockheed Martin Sippican was fined $3 million for continuing to provide technical data and support to BAE Australia as part of the Nulka project over a four-month period between its Technical Assistance Agreement expiring and its new agreement coming into effect.[213] Even more concerning was that Lockheed Martin Sippican was complying with the requirements

---

[206] See, for example Adam Grissom, 'The Future of Military Innovation Studies', *Journal of Strategic Studies*, Vol. 29, No. 5, October 2006; and Michael C. Horowitz and Shira Pindyck, 'What Is a Military Innovation and Why It Matters,' *Journal of Strategic Studies*, Vol. 46, No. 1, February 2023.

[207] Jon Ludwigson, *Directed Energy Weapons: DOD Should Focus on Transition Planning*, Government Accountability Office, GAO-23-105868, 2023.

[208] Gambling, Crozier, and Northam, 2023.

[209] Gambling, Crozier and Northam, 2013.

[210] This review is the 1986 *Review of Defence Capabilities*. The review was a watershed report in the Australian defence ecosystem. Among other responses, the Australian Government rationalised and privatised Australia's munitions and explosives industries, which had a direct impact on this project (Gambling, Crozier and Northam, 2013).

[211] *Nulka* is an Australian Aboriginal word that means 'be quick' (Gambling, Crozier and Northam, 2013).

[212] Gambling, Crozier and Northam, 2013.

[213] John Black, 'Lockheed Martin Fined $3 Million Civil Penalty for Violations of Subsidiary Sippican', *Export Compliance Training Institute*, 28 January 2007.

of its contract with U.S. Navy by continuing to provide this support to the Australian side of the manufacturing line.[214] This case relates to the concerns we heard from interviewees about data-sharing and intellectual property ownership; one interviewee specifically declared their concern that a country or firm might not be able to get back data or intellectual property that it contributed to a co-developed project, as happened in the Nulka case.

Full-scale development officially began on the Australian side on the 16 January 1988. A notable challenge during this phase was frequent changes in the senior leadership in both the Australian and U.S. project offices. For example, there were five program directors in Canberra between January 1988 and March 1991, one of whom only lasted a single month in the position. On the U.S. side, the Navy Captain leading the project office changed every 18 months.[215] These changes undermined the program's capacity to build momentum or sustain a singular leadership vision. Fortunately, there was some consistent leadership (e.g. the civilian U.S. program manager). A production contract was not signed to supply RAN, the U.S. Navy and the Canadian Navy until 1997.[216]

[214] James E. Bartlett III, J. Daniel Chapman, Kay C. Georgi, Ira E. Hoffman and Adam Klauder, 'Export Controls and Economic Sanctions', *International Lawyer*, Vol. 42, No. 2, 2007.

[215] Gambling, Crozier and Northam, 2013.

[216] Gambling, Crozier and Northam, 2013.

Chapter 6. Illustrative Potential Use Cases for Military AI Cooperation

Because of the potentially significant challenges—legal, operational, ethical, and technical—posed by systems with lethal capabilities and high levels of autonomy, it is also worth considering the following potential uses cases for co-design of military AI.

Military Artificial Intelligence for Humanitarian Aid and Disaster Relief

One option for military AI would be to focus AUKUS AI co-development initiatives on systems that are intended for no-combat environments in which there is clear alignment among the partners on the system's intended use and outcomes, such as humanitarian assistance and disaster response (HA/DR) operations. These types of operations, although they typically represent a small segment of a military's total activities, can involve significant investments and capabilities. For example, in response to record monsoon rains that devastated Pakistan in 2010, DoD contributed about $54 million through the transport of 11,000 metric tons of relief supplies; evacuation of 26,000 people stranded by flooding; donation of 450,000 humanitarian daily rations; and provision of various prefabricated bridges.[217] Climate change—with its potential to increase the risk of natural disasters and associated challenges such as disease outbreak, famine, and population displacement—will likely place additional demands on militaries in the near future. AI could position the AUKUS militaries to carry out HA/DR operations more effectively, particularly as a multinational force.

AI for HA/DR operations is a new but expanding field. Examples of HA/DR AI applications include natural language processing of Twitter and other social media data to identify where communities have been affected by a natural disaster and the severity of the impact.[218] HA/DR AI applications could also include using object recognition on satellite images to detect damage to buildings or other infrastructure and using predictive analytics to determine the optimal allocation of humanitarian resources using meteorological data and market analysis.[219] A key limitation of these applications is that they are heavily reliant on available data, which might not be reliable, and might even be systematically biased.[220] For example, there might be fewer satellite images of remote, less affluent areas compared with

---

[217] Jennifer D. P. Moroney, Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, and Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, RAND Corporation, RR-146-OSD, 2013.

[218] Ryan-Mosley, Tate, 'How AI Can Be Helpful in Disaster Response', *MIT Technology Review*, 20 February 2023.

[219] Ryan-Mosley, 2023; Wenjuan Sun, Paolo Bocchini, and Brian D. Davison. 'Applications of artificial intelligence for disaster management.' *Natural Hazards*, Vol. 103, No. 3, 2020.

[220] Ana Beduschi 'Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks', *International Review of the Red Cross*, No. 919, June 2022.

more-urbanised, more-affluent areas, which could potentially result in the underrepresentation of more-vulnerable communities in disaster preparation, response and recovery efforts.[221] In such a case, a multinationally developed and operated object recognition tool that integrates open-source images with images collected from UK, Australian and U.S. drones and military satellites could fill gaps in otherwise siloed individual country systems and enable the AUKUS partners to respond to disasters in a more fair and effective way.

Cyber Cooperation

The AUKUS partners cooperate on cyberspace issues through a variety of fora and multiple mechanisms. These avenues include military discussions on operational cyber issues, intelligence-sharing through Five Eyes,[222] diplomatic discussions about cyber policy and technical information sharing through Computer Security Incident Response Teams.[223] In addition, the partners have collaborated on multiple operational activities, such as conducting combined attribution of malicious activity and law enforcement cooperation to investigate and prosecute cyber criminals.[224] In these cases, the shared approach has promoted operational outcomes and bolstered a set of shared approaches and norms of behaviour in cyberspace.

This cooperation has proceeded despite divergences in domestic approaches to cybersecurity, domestic law and each state's respective interpretations of international law and suggests that there could be a way ahead for more robust cooperation on other emerging technologies. Although the states might have some differences in interpretation of international law, there is also a foundation of values and a stated commitment to human rights that has anchored shared approaches to cyberspace collaboration.[225] One key element is that cyber cooperation is integrated across many channels—from senior level policy discussions to technical cyber forensics and information-sharing—and pervades many policy areas. AI cooperation might similarly need to be integrated throughout a variety of mechanisms to provide a foundation for more-sensitive collaboration in operational military contexts.

AI stands to have a major impact on cybersecurity both by potentially improving attackers ability to exploit vulnerabilities and by enabling defenders to identify vulnerabilities for patching and detect anomalous behaviour in networks that derive from a malicious

---

[221] See, for example, Beduschi 2022; and Ryan-Mosley2023.

[222] Dennis Desmond, 'The Highly Secretive Five Eyes Alliance Has Disrupted a China-Backed Hacker Group—in an Unusually Public Manner', *The Conversation*, 26 May 2023.

[223] University of Queensland Cyber and AUSCERT, *Joint Submission—Discussion Paper 2023-2030 Australian Cyber Security Strategy*, 12 April 2023.

[224] Desmond, 2023.

[225] White House, 'Australia-United States Joint Leaders' Statement—An Alliance for Our Times', press release, 20 May 2023

source.[226] Although it is not clear whether AI will favour offensive or defensive cyber applications, it is safe to say that AUKUS countries will need to be aware of how adversaries might leverage AI for cyberattacks and be prepared to defend themselves and each other. In this way, there could be opportunities for these countries to leverage existing cybersecurity cooperation across various channels to improve their ability to use AI across cybersecurity applications. Some elements of this cooperation might involve collaborative efforts to use AI to conduct penetration testing and red-teaming of military networks (e.g. through use of generative AI for vulnerability discovery)[227] or to rewrite malware to evade detection.[228]

Computer Vision

Cooperation between the AUKUS partners on computer vision algorithms comes with some obvious advantages and some obvious potential pitfalls. One substantial advantage to this focus area would be the prior experience of DoD with Project Maven.[229] While Maven did not include international partners, it was deliberately operated in a secure unclassified environment to allow work with private sector companies that had not traditionally been defence contractors and to allow for the inclusion of employees from those companies who had not received a security clearance.[230] If DoD can learn to work with these kinds of new partners, it should be able to learn to work with its most trusted allies on AI algorithms.

Selecting computer vision as a focus area would resolve some of the major challenges that inhibit collaboration on AI. Computer vision has clear applications to many intelligence functions and warfighting needs: It would quickly answer the question 'AI for what?' Additionally, computer vision algorithms are relatively easier to test and evaluate compared with other types of AI algorithms—military personnel and intelligence analysts can look at the outputs of these algorithms and determine whether they are correctly identifying objects of interest. The close intelligence relationship between the AUKUS partners and established trust each has earned as a member of Five Eyes should also reduce some of the difficulties inherent to data-sharing and collaboration on these issues.

However, any collaboration on computer vision would involve some difficulties. Ideally, allies and partners would invest in data pipelines that generate clean, labelled datasets owned by the government. As Lt. Gen. John Shanahan, the first director of Project Maven, put it

---

[226] Max Heinemeyer, 'Hafnium Cyber-Attack Neutralized by AI in December 2020', Darktrace blog, 15 April 2021.

[227] Andrew Lohn, Anna Knack, Ant Burke and Krystal Jackson, *Autonomous Cyber Defense: A Roadmap from Lab to Ops*, Center for Emerging Technology and Security, June 2023.

[228] Lily Hay Newman, 'NSA Cybersecurity Director Says "Buckle Up" for Generative AI', *Wired*, 27 April 2023.

[229] Launched in 2017, Project Maven is a DoD initiative focused on leveraging commercial innovations in AI-based image processing and recognition software for UAV surveillance operations.

[230] Gregory Allen, 'Project Maven Brings AI to the Fight Against ISIS', *Bulletin of the Atomic Scientists*, 21 December 2017.

'data is at the heart of every AI project'.[231] One important lesson from DoD's experience with Maven was the need to maintain government ownership of the data at every step of the process.[232] If all data are owned by the participating governments, some of the major barriers that have hampered other co-development R&D projects could be reduced or even eliminated. In particular, data owned by DoD (as opposed to data owned by contractors who are doing work for DoD) could be shared with allies and partners at the direction of the DoD organization that owns it without the need for a separate ITAR review conducted by the State Department. We argue that this could resolve one of the greatest potential concerns of the closest U.S. allies about the co-development of technology with the United States.

Additionally, although the United States, United Kingdom and Australia have a history of sharing intelligence data, they do not have the same extensive history of sharing compute and storage resources or aligning data pipelines, data labels and data standards.[233] Establishing these operational routines would require time and effort. Divergent cybersecurity standards could prove to be a substantial burden on collaboration over AI. Many of the tools and libraries that private-sector software engineers and data scientists rely on have not passed DoD's often time-consuming cybersecurity reviews and thus have not received an 'authority to operate' on DoD systems. Without careful forethought, expanding the number of partners and cybersecurity review processes that collaborative AI projects are required to complete could make this problem substantially worse.

Finally, integrating AI and computer vision algorithms into a military kill chain could generate ethical controversies. Project Maven notably sparked a backlash at Google when employees found out their employer was participating in the program.[234] Each of the AUKUS partners would have to weigh the potential for a domestic backlash if any of their international collaborators used technology that had been co-developed in a way that their publics considered to be a breach of ethnical norms. However, the AUKUS partners' high-level alignment to AI ethics principles suggests that they could undertake a coordinated and calibrated approach to assessing the benefits and risks of this cooperation.

---

[231] Joint Artificial Intelligence Center, 'Lt. Gen. Jack Shanahan Media Briefing on AI-Related Initiatives within the Department of Defense', Chief Digital and Artificial Intelligence Board, blog, 30 August 2019.

[232] Sydney Freedberg, 'Exclusive: Pentagon's AI Problem is 'Dirty' Data: Lt Gen. Shanahan', *Breaking Defense*, 13 November 2019.

[233] Christianson, Monaghan and Cooke, 2023.

[234] Scharre, 2023.

Chapter 7. Core Recommendations

In this chapter, we present our core recommendations for AUKUS co-design and co-development of AI.

Prioritise and Streamline Approaches to Ethically and Legally Responsible Artificial Intelligence

One way to overcome the challenges and facilitate collaboration and co-production of AI is to coordinate approaches to responsible military AI development and deployment. Doing so will help build trust among AUKUS parties while also demonstrating for broader audiences how AI can be used responsibly. Thereby, public support and further opportunities for partnership with additional operational partners and commercial vendors can be developed.

Although there are some divergences among AUKUS states in the articulation of ethical principles, and long-standing subtle differences in how the states interpret their legal responsibilities and weapon reviews, our analysis found that the partners have significant commonalities to ethical deployment of AI. As AI advances and the countries develop more experience, there will be opportunities to further streamline a shared approach to the implementation of AI ethics principles. A few specific areas of cooperation that will further shape responsible approaches to military AI and demonstrate a commitment to ethical principles include the following:

- Leveraging the National Institute of Standards and Technology's AI Risk Management Framework and other developing approaches for AI risk to integrate AI risk assessment into the military AI life cycle.[235]
- Combined AI red-teaming to identify AI risks and other vulnerabilities.
- Shared public articulation of legal assessments of AI technologies demonstrating commitment to international legal principles and robust implementation into military practice.
- Development of shared processes for approving technologies in high stakes applications (such as those in dense operational settings or with lethal payloads), including senior-level review standards and accountability mechanisms.
- Development of processes to engage external stakeholders, such as independent AI researchers working on such topics as bias and discrimination in AI systems and such humanitarian organizations as the International Committee of the Red Cross.
- Additional public events and statements to further display common approaches and invite additional insight into how AI can be used responsibly.

[235] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, U.S. Department of Commerce, January 2023.

Create New Multinational Research and Development Centres

It is also important that AUKUS states, individually and in partnership, continue to develop their R&D capabilities in this space. One option would be to establish new multinational R&D centres, for example a multinational laboratory operating under a type of joint Federally Funded Research and Development Center model. Alternatively, an existing mechanism, such as The Technical Cooperation Program, could be leveraged to provide a common forum for collaborative research.

Regardless of the chosen mechanism, AUKUS research collaboration towards military AI should be guided by three principles. The first is a commitment to generating common benchmarks and standards among member states. This commitment would include such measures as the establishment of shared data standards, data pooling methods, export control waivers and developing shared TEV&V processes and ranges. Secondly, and relatedly, the research efforts should be specialised and genuinely multinational, with individual project leadership assigned on a best athlete basis. Doing so would allow AUKUS members to concentrate their resources, build on the success of Australia and the UK on key niche capabilities and generate efficiencies. Finally, combined research centres should be established under a model that enables cooperation with the private sector, particularly smaller and otherwise nontraditional defence firms. Taking these three factors into account, we recommend that the AUKUS states integrate their defence innovation efforts related to AI, recognise and support the niche strengths of junior partners and leverage lessons from the commercial sector, potentially by embedding experienced end-users into a newly established AUKUS AI collaborative research hub, in the same manner as the UK's J-Hub program.[236]

Integrate Data and Artificial Intelligence into Multinational Exercises

One mechanism that could be essential for collaboratively developing AI would be to develop AI applications in an iterative manner and integrate them into joint exercises between the collaborators. This mechanism would yield several benefits. First, aligning the use cases for AI with practical tasks included in the exercises would ensure that these use cases are relevant to the warfighter and deliver real value. Second, combined exercises would be an invaluable opportunity to gather feedback directly from the operators to help the engineering team develop these applications in an iterative manner. Finally, these exercises would act as 'training exercises' for military data and ensure that datasets from the various partners are interoperable and effective.[237] Using data to support actual military activities is the only way to ensure that it will be ready for the fight. As Schuyler Moore, Chief

[236] Daniel Kliman and Brendan Thomas-Noone, 'How the Five Eyes Can Harness Commercial Innovation', *Defense One*, 25 July 2018.

[237] Ryseff, 2020.

Technology Officer of U.S. Central Command, notes 'when it comes to digital warfare, practice makes perfect and we cannot begin practicing soon enough'.[238]

AUKUS members have already begun to move towards multinational exercises and research activities, and these efforts should be expanded. For example, on 28 April 2023, there was a successful multinational trial, involving both military and civilian personnel, of aerial and ground vehicles and the interchange of AI models and AI-enabled assets operating in a swarm to detect and track targets.[239] This trial, 'organised by the UK's Defence Science and Technology Laboratory (Dstl), reportedly achieved variety world firsts, including the live retraining of models in flight and the interchange of AI models between AUKUS nations. The AUKUS collaboration is looking to rapidly drive these technologies into military capabilities'.[240] According to Hugh Jeffrey, Deputy Secretary Strategy, Policy and Industry Group, the trial 'exemplified the determination of AUKUS partners to rapidly translate disruptive technologies into capability' and demonstrated that 'AUKUS can deliver a capability that is greater than what any one country can do alone'.[241]

Collaboratively Develop Compatible Operational Concepts for the Use of Military Artificial Intelligence

Beyond the technical barriers, translating systems co-developed under AUKUS into disruptive military capability requires that participating militaries agilely and collaboratively develop operational concepts to guide their integration of such systems. Although it is relatively rare for militaries to jointly develop operational concepts, the UK and Australian militaries have both previously demonstrated the capacity to successfully emulate concepts developed by the United States. The core of this challenge is how to integrate operational requirements for a given system (which might be different across AUKUS states) into the design process in such a manner that the resulting system meets those needs while remaining interoperable. We propose that there are three key policy actions that could be taken to overcome these challenges. The first would be to develop a shared data collection and storage ecosystem that draws data from, and can be accessed by, each of the AUKUS states. This system could be leveraged, along with the data produced by following the previous recommendation, to develop a shared (or interactable) synthetic training environment in which to develop machine learning AI-based systems. AUKUS states could also expand opportunities for collaborative doctrinal development, whether through exercises, multinational wargaming or the establishment of a professional journal. Finally, we recommend that AUKUS militaries consider developing intra-organizationally standardised

[238] Schuyler Moore, 'To Prepare for Digital Warfare the Military Must Run More Digital Exercises', 8 February 2023.

[239] Lauren Kahn, 'AUKUS Explained: How Will the Trilateral Pact Shape Indo-Pacific Security?' Council on Foreign Relations, last updated 12 June 2023; UK Ministry of Defence, and Defence Science and Technology Laboratory, 'World First as UK Hosts Inaugural AUKUS AI and Autonomy Trial', press release, 26 May 2023.

[240] UK Ministry of Defence, and Defence Science and Technology Laboratory, 2023.

[241] Australian Department of Defence, 'AUKUS Partners Demonstrate Advanced Capabilities AI Trial', press release, 26 May 2023.

definitions, operational benchmarks and training mechanisms for both the AI systems themselves and the humans that are asked to serve alongside them.

Explore Mechanisms for Greater Innovation Ecosystem Integration

Among the opportunities offered by AUKUS Pillar Two are those related to leveraging the strengths and niche capabilities of each partner's innovation ecosystem. The most innovative and inventive aspects of AUKUS Pillar Two and the commercialisation of the associated technologies will not be government driven but will take place within and between private companies, research organisations and universities across the United States, the UK and Australia. Indeed, while defence and tech primes will continue to have a significant role, because they possess the capability platforms and are working within significant budgets to ensure that the platforms are appropriate to need, AUKUS members will likely continue to rely on startups and subject-matter experts to push disruptive innovations. These actors should, therefore, be incentivised and supported as a source of both innovation and an incubator for 'a highly skilled workforce through the exchange of technology and skilled workers'.[242]

Equally, the AUKUS states should take steps to capitalise on the attractiveness of their societies and structures to attract top-tier talent and to allow for that talent to move freely within the alliance. The free movement of a highly skilled AUKUS workforce across military, civilian and industry sectors would enable cross-pollination and augmentation of the requisite expertise. Effective leveraging of this expertise could be achieved through 'a specialised AUKUS visa to ease collaboration and movement. This would also allow for the free exchange of ideas across industry workers, raising the level of expertise in many advanced-technology areas across the partnership'.[243] Under the existing system, security clearance waivers, although necessary for co-development of sensitive technologies, are subject to even slower and more complex processes than achieving citizenship.

Implement the 'ITAR-Free Zone,' or the Maven Model

One way to address some of the concerns we heard from our interviews with AI experts from top allies would be to adapt the model used in Project Maven to encompass U.S. allies and partners. Although Maven's unique status as a pathfinder project empowered by senior DoD leaders would be hard to replicate, several of the key principles behind Maven's approach could prove equally valuable to effectively co-developing AI among allies and partners.

Identifying a concrete initial use case to focus on in consultation with key allies and partners could spur progress. Many potential collaborators have yet to establish specific priorities for AI tied to practical use cases that would benefit their militaries. Helping these

[242] Jason Van der Schyff, 'AUKUS Will Redefine Government–Industry Partnerships', *The Strategist*, 21 February 2023.

[243] Christianson, Monaghan and Cooke, 2023.

partners move beyond vague and aspirational plans and establish clear, practical use cases for AI could play a substantial role in breaking down these barriers.

Additionally, concerns about intellectual property rights could prevent allies and partners from collaborating with DoD to develop AI algorithms. DoD could reassure its partners and allies that their intellectual property rights will be respected in two ways. First, past experience has left many potential collaborators with the perception that ITAR will be a major barrier for these projects. If DoD wants to address these concerns, it might mimic Project Maven's approach to data ownership. In Maven, the U.S. government maintained ownership of the data at all stages. DoD handled the original collection of data from intelligence, surveillance and reconnaissance assets, and the data were labelled under the direction of Maven personnel. Private-sector corporations focused on training AI algorithms using the data provided by the government. If DoD followed this model, allies and partners would not need to worry about ITAR issues for data; because the data would be government owned, there would be no question that the government can choose to share it. Similarly, the U.S. government would have no claim on the original data shared by allies and partners if those allies and partners owned the data themselves and invested in labelling it for use by AI algorithms.

Second, replicating Maven's approach to intellectual property rights could alleviate some of the greatest concerns of potential collaborators. Companies that participated in Maven owned any intellectual property they generated—in this case, the AI algorithms their engineers and researchers trained. However, the U.S. government received a permanent license to use an AI algorithm developed under Maven. Even if contractors decided to end their participation in the project, the government could continue to use any AI models they had developed prior to their exit. A similar arrangement would extend similar rights to any foreign collaborators; all the collaborators in the co-development of AI could receive a permanent license to use any algorithms resulting from the collaboration while any company training AI models would own the intellectual property they create. Although this approach would not resolve all questions related to intellectual property concerns—in particular, it would not address whether AI models collaboratively developed could be exported to nonparticipating nations—it could address some of the largest questions.

Finally, DoD could consider establishing shared infrastructure to support the co-development of AI projects. One significant step it could take would be to establish multinational funded cloud computing environments to be used for data analytics and AI projects. AUKUS-operated data centres of this type would allow the United States and its close allies and partners to benefit from economies of scale when building up the infrastructure necessary to develop advanced AI algorithms. AI algorithms require very significant investments in computational resources and storage capacity. Pooling these investments would allow each of the participants to take advantage of the full compute power purchased on a rotational basis (i.e. each participant receives an equitable proportion of compute time). This approach would be similar to how large technology companies typically share their cloud computing resources among their divisions. While this recommendation would require significant policy changes to implement and would likely face significant

cultural resistance, it would not be conceptually different from the current mechanisms the United States uses to share data with its allies and partners. The key challenges and recommendations explored in this report are summarised in Tables 7.1, 7.2, and 7.3.

Table 7.1. Challenges and Recommendations: Leverage Strengths of Each Partner While Preserving the Perspective and End Value of the Product to Junior Partners

Challenges	Recommendations
Conceptual problems	• Consider AI capabilities that provide a clear use case for military activities, such as – large language models for analysing open sources to identify for intelligence and command and control – object recognition for strategic or joint intelligence, surveillance and reconnaissance and strike – predictive analytics to determine the optimal allocation of maintenance and logistics activities during a co-developed system's life of type. • Use AI-enabled command and control assistant systems for operational command posts.
Distinct operational considerations	• Align norms governing the use of AI in military operations. • Use combined exercises to identify and address any meaningful differences in operational considerations. • Develop shared training standards and exercises. • Develop an intra-AUKUS agreement on benchmarks for key terms, including meaningful human control.
Partnership challenges	• Embed sovereign protections in the production and development processes, which could be achieved through early assignment of research lines of effort on a best athlete basis. • Carve out exemptions or rapid approval pathways for firms involved in AUKUS Pillar Two technology co-development, potentially including the suspension of 'ITAR taint'. • Leverage and expect existing Five Eyes and AUKUS technology collaboration mechanisms. • Increase U.S. commitment to friend-shoring maintenance and production capabilities to AUKUS allies where they are developing niche specialization.

Table 7.2. Challenges and Recommendations: Developing and Integrating Ethically and Legally Responsible Artificial Intelligence

Challenges	Recommendations
Ambiguity around implementing the AI ethics principles	• Collaborate on a shared framework for operationalising AI ethics principles, for example, through the AUKUS AI Working Group. The framework could include, – guidance on engaging community stakeholders to identify potential areas in which AI could contribute to bias and discrimination – approaches to testing and evaluating algorithmic models to enhance reliability – procedures for individuals who are affected by the technology (such as aid recipients) to challenge automated decisions to foster accountability – mechanisms for avoiding and mitigating breaches to data privacy.
Differing approaches to the legal review process	• Collaborate on the development of a compatible legal review process for military applications of AI. • Develop common definitions and function-based standards for emergent AI-enabled systems.

Table 7.3. Challenges and Recommendations: Practical Aspects of Enabling Cooperation Across Barriers

Challenges	Recommendations
Sharing data and infrastructure	• Develop appropriate contracting mechanisms that facilitate data sharing, avoid vendor lock-in and enable intra-AUKUS export exemptions. • Address regulatory barriers to data sharing (GDPR, MOUs). • Align data standards and cybersecurity requirements.
Limited testing and evaluation capabilities	• Develop shared synthetic training environments. • Consider creating exchange programs for training and experience personnel. • Conduct multinational exercises to socialise norms, generate common understanding and capture training data.
Stringent export controls	• Consider an AUKUS-level agreement for the reduction or removal of ITAR barriers to co-development programs. This step could be paired with mutual recognition and development of information security and classification protocols. • Identify a concrete initial use case to focus on in consultation with key allies and partners as a test case for lowering export restrictions. • Replicate Project Maven's approach to intellectual property rights and cross-national collaboration on identified task-based focus areas. • Consider establishing shared infrastructure to support the co-development of AI projects, including secured common cloud environments.

Abbreviations

ADF	Australian Defence Force
AI	artificial intelligence
AUKUS	Australia, United Kingdom, and United States
CTO	Chief Technology Officer
DCDC	Development, Concepts and Doctrine Centre
DIU	Defence Innovation Unit
DoD	U.S. Department of Defense
DOSL	Directorate Operations and Security Law
DSTG	Defence Science and Technology Group
FCAS	Future Combat Air System
HA/DR	humanitarian assistance and disaster response
IHL	international humanitarian law
ITAR	International Traffic in Arms Regulations
LAWS	lethal autonomous weapon systems
MOU	memorandum of understanding
NATO	North Atlantic Treaty Organization
NTIB	National Technology and Industrial Base
R&D	research and development
RAN	Royal Australian Navy
RDT&E	research, development, test, and evaluation
TEV&V	test, evaluation, verification, and validation
UCAV	unmanned combat aerial vehicle
UK	United Kingdom

References

Alexander, Michael, and Timothy Garden, 'The Arithmetic of Defence Policy', *International Affairs*, Vol. 77, No. 3, July 2001.

Allen, Gregory, 'Project Maven Brings AI to the Fight Against ISIS', *Bulletin of the Atomic Scientists*, 21 December 2017.

Austal to Undertake Patrol Boat Autonomy Trial for RAN', Australian Defence Magazine, 7 October 2022.

Australia, Canada, Japan, Republic of Korea, United Kingdom and United States, *Draft Articles on Autonomous Weapon Systems—Prohibitions and Other Regulatory Measures on the Basis of International Humanitarian Law ('IHL')*, United Nations, 13 March 2023.

'The Australian Article 36 Review Process', Second Session, *Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious*, 27–31 August 2018

Australian Defence Science and Technology Group, 'Nulka Active Missile Decoy', webpage, Australian Department of Defence, undated. As of 15 December 2023: https://www.dst.defence.gov.au/innovation/nulka-active-missile-decoy

Australian Defence Science and Technology Group, 'How the Falklands War gave rise to Australia's Prize Defence Export—After Years of Struggling with Reluctance', 6 May 2022.

Australian Department of Defence, 'The Technical Cooperation Program', webpage, undated. As of 15 December 2023: https://www.dst.defence.gov.au/partnership/technical-cooperation-program

Australian Department of Defence, *Defence Legal Review of New Weapons Guide*, 2020

Australian Department of Defence, *National Defence: Defence Strategic Review*, 2023.

Australian Department of Defence, 'AUKUS Partners Demonstrate Advanced Capabilities AI Trial', press release, 26 May 2023.

Australian Department of Industry, Science and Resources, *Australia's Artificial Intelligence Ethics Framework*, 7 November 2019.

BAE Systems, 'Nulka Active Missile Decoy', webpage, undated. As of 15 December 2023: https://www.baesystems.com/en-aus/what-we-do/nulka

Bartlett III, James E., J. Daniel Chapman, Kay C. Georgi, Ira E. Hoffman and Adam Klauder, 'Export Controls and Economic Sanctions', *International Lawyer*, Vol. 42, No. 2, 2007

Bassi, Justin, ‘Why the AUKUS Partnership Is About Much More Than Warfighting’, *The Hill*, 23 October 2023.

Beduschi, Ana, ‘Harnessing the Potential of Artificial Intelligence for Humanitarian Action: Opportunities and Risks’, *International Review of the Red Cross*, No. 919, June 2022.

Béraud-Sudreau, Lucie, Xiao Liang, Diego Lopes da Silva, Nan Tian and Lorenzo Scarazzato, ‘The SIPRI Top 100 Arms-Producing and Military Services Companies, 2021’, Stockholm International Peace Research Institute, December 2022.

Black, John, ‘Lockheed Martin Fined $3 Million Civil Penalty for Violations of Subsidiary Sippican’, *Export Compliance Training Institute*, 28 January 2007

Boulanin, Vincent, and Maaike Verbruggen, *SIPRI Compendium on Article 36 Reviews*, Stockholm International Peace Research Institute, 2017.

Bronk, Justin, ‘FCAS: Is the Franco-German-Spanish Combat Air Programme Really in Trouble?’ Royal United Services Institute, 1 March 2021.

Carouso, James, Thomas Schieffer, Jeffrey Bleich, John Berry and Arthur Culvahouse, ‘ITAR Should End for Australia’, Center for Strategic and International Studies, 7 December 2022.

Chakravorti, Bhaskar, Ajay Bhalla, Ravi Shankar Chaturvedi and Christina Filipovic, ‘50 Global Hubs for Top AI Talent’, *Harvard Business Review*, 21 December 2021.

Christianson, John, Sean Monaghan and Di Cooke, *AUKUS Pillar Two: Advancing the Capabilities of the United States, United Kingdom, and Australia*, Center for Strategic and International Studies, 2023.

Cochrane, Jared M., ‘Conducting Article 36 Legal Reviews for Lethal Autonomous Weapons’, *Journal of Science Policy and Governance*, Vol. 16, No. 1, 13 April 2020.

Cole, Matthew, *Code Over Country: The Tragedy and Corruption of SEAL Team Six*, Public Affairs, 2022

Corben, Thomas, ‘AUKUS: A Year On—What to Make of AUKUS After 365 Days?’ Royal United Services Institute of New South Wales, 23 November 2022.

DCDC—*See* Development, Concepts and Doctrine Centre.

Defence Member and Family Support, *Overseas Lateral Recruitment: Defence Member and Family Support*, Australian Department of Defence, 2016.

Desmond, Dennis, ‘The Highly Secretive Five Eyes Alliance Has Disrupted a China-Backed Hacker Group—in an Unusually Public Manner’, *The Conversation*, 26 May 2023.

Development, Concepts and Doctrine Centre, *UK Weapon Reviews*, 2016.

DeVore, Marc R., ‘International Armaments Collaboration and the Limits of Reform’, *Defence and Peace Economics*, Vol. 25, No. 4, August 2014.

DoD—*See* U.S. Department of Defense.

Dossi, Amos, and Niklas Masuhr, 'European Fighter Programs: A Preliminary Assessment', *CSS Analyses in Security Policy*, Vol. 291, October 2021.

DSTG—*See* Defence Science and Technology Group.

European Forum on Armed Drones, 'Germany', webpage, undated-a. As of 15 December 2023 https://www.efadrones.org/countries/germany/

European Forum on Armed Drones, 'Spain', webpage, undated-b. As of 15 December 2023: https://www.efadrones.org/countries/spain/

Foreign Affairs Committee, *Tilting Horizons: The Integrated Review and the Indo-Pacific*, Eighth Report of Session 2022–23, UK Parliament, 20 August 2023.

Freedberg, Sydney, 'Exclusive: Pentagon's AI Problem is "Dirty" Data: Lt Gen. Shanahan', *Breaking Defense*, 13 November 2019.

Gaida, Jamie, Jennifer Wong-Leung, Stephanie Robin and Danielle Cave, *ASPI's Critical Technology Tracker: AUKUS Updates*, Australian Strategic Policy Institute, last updated 22 September 2023.

Gambling, David, Mal Crozier and Don Northam, *Nulka: A Compelling Story: Ingenuity, Partnership, Perseverance*, Australian Department of Defence, 2013.

'Germany to Get Weaponized Drones for the First Time', *Defense Post*, 6 April 2022.

Government of Canada, *Key Events That Shaped the Controlled Goods Program*, last updated 05 November 2019.

Greenwalt, William, *Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies*, Scowcroft Center for Strategy and Security, 2019.

Greenwalt, William, and Tom Corben, *Breaking the Barriers: Reforming US Export Controls to Realise the Potential of AUKUS*, United States Studies Centre at the University of Sydney, 2023.

Grissom, Adam, 'The Future of Military Innovation Studies', *Journal of Strategic Studies*, Vol. 29, No. 5, October 2006.

Harris, Bryant, 'AUKUS Standoff: Australia, UK Wait on Congress to Approve Pact', *Defense News*, 5 September 2023.

Haugh, Brian A., David A. Sparrow, and David M. Tate, *The Status of Test, Evaluation, Verification, and Validation (TEV&V) of Autonomous Systems*, Institute for Defense Analyses, September 2018.

Hay Newman, Lily, 'NSA Cybersecurity Director Says "Buckle Up" for Generative AI', *Wired*, 27 April 2023.

Heinemeyer, Max, 'Hafnium Cyber-Attack Neutralized by AI in December 2020', Darktrace Blog, 15 April 2021.

Hellyer, Marcus, *Cracking the Missile Matrix: The Case for Australian Guided Weapons Production*, Australian Strategic Policy Institute, 2021.

Hoffman, Wyatt, *AI and the Future of Cyber Competition*, Center for Security and Emerging Technology, 2021.Jackett, Jennifer, *Laying the Foundations for AUKUS: Strengthening Australia's High-Tech Ecosystem in Support of Advanced Capabilities*, United States Studies Centre at the University of Sydney, 2022.

Horowitz, Michael C., and Shira Pindyck, 'What Is a Military Innovation and Why It Matters,' *Journal of Strategic Studies*, Vol. 46, No. 1, February 2023.

International Committee of the Red Cross, 'Article 36—New Weapons', webpage, undated. As of 15 December 2023: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36

Jackett, Jennifer, *Defence Innovation and the Australian National Interest*, Defence and Security Institute, University of Western Australia, 2023.

Jennings, Peter, *AUKUS: New Opportunities for the United States and its Closest Allies*, Heritage Foundation, 18 October 2022.

Joint Artificial Intelligence Center, 'Lt. Gen. Jack Shanahan Media Briefing on AI-Related Initiatives within the Department of Defense', Chief Digital and Artificial Intelligence Board, blog, 30 August 2019.

Kahn, Lauren, 'AUKUS Explained: How Will the Trilateral Pact Shape Indo-Pacific Security?' Council on Foreign Relations, last updated 12 June 2023.

Kerr, Julian, and Andrew MacDonald, 'Australia's 2022–23 Defence Budget Climbs by 7.4%', *Janes Defence News*, 30 March 2022.

Kliman, Daniel, Ben FitzGerald, Kristine Lee and Joshua Fitt, *Forging an Alliance Innovation Base*, Center for a New American Security, 2020.

Kliman, Daniel, and Brendan Thomas-Noone, 'How the Five Eyes Can Harness Commercial Innovation', *Defense One*, 25 July 2018.

Lin-Greenberg, Erik, 'Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making', *Texas National Security Review*, Vol. 3, No. 2, Spring 2020.

Lohn, Andrew, Anna Knack, Ant Burke and Krystal Jackson, *Autonomous Cyber Defense: A Roadmap from Lab to Ops*, Center for Emerging Technology and Security, June 2023.

Ludwigson, Jon, *Directed Energy Weapons: DOD Should Focus on Transition Planning*, Government Accountability Office, GAO-23-105868, 2023.

Mauri, Diego, 'The Holy See's Position on Lethal Autonomous Weapons Systems: An Appraisal Through the Lens of the Martens Clause', *Journal of International Humanitarian Legal Studies*, Vol.11, No.1, 2020.

McGinn, John G., and Michael T. Roche, *Developing a 'Build Allied' Approach to Increasing Industrial Base Capacity*, Naval Postgraduate School, 1 May 2023.

Moore, Schuyler, 'To Prepare for Digital Warfare the Military Must Run More Digital Exercises"' *Breaking Defense*, 8 February 2023.

'More Work Needed on AUKUS Technology Sharing—British, Australian Officials', Reuters, 2 March 2023.

Moroney, Jennifer D. P., and Alan Tidwell, 'Making AUKUS Work', *RAND Blog*, 22 March 2022. As of 15 December 2023: https://www.rand.org/blog/2022/03/making-aukus-work.html

Moroney, Jennifer D. P., Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom and Abby Doll, *Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region*, RAND Corporation, RR-146-OSD, 2013. As of 15 December 2023: https://www.rand.org/pubs/research_reports/RR146.html

National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, U.S. Department of Commerce, January 2023.

Nemeth, Bence, 'Military Innovation and Capability Development in a Multinational Context: The Costs and Benefits of Multinational Cooperation', *Air Power Journal*, Fall 2022.

Obecny, Kristina, Gregory Sanders, Janes Ruedlinger and Jesse Ellman, *'U.S.–Canadian Defense Industrial Cooperation*', Center for Strategic and International Studies, June 2017.

Oswald, Rachel, 'Lawmakers Seek to Ease Defense Export Controls to UK, Australia', Roll Call, 23 May 2023.

Poitras, Ryan, 'Article 36 Weapons Reviews and Autonomous Weapons Systems: Supporting an International Review Standard', *American University International Law Review*, Vol. 34, 2018.

Robson, Seth, 'Job Pool Expanding for US Troops Interested in Heading Down Under', *Stars and Stripes*, 1 April 2014.

Ryan-Mosley, Tate, 'How AI Can Be Helpful in Disaster Response', *MIT Technology Review*, 20 February 2023.

Ryseff, James, 'The United States Can Only Achieve AI Dominance with Its Allies', *War on the Rocks*, 9 October 2020.

Ryseff, James, Eric Landree, Noah Johnson, Bonnie Ghosh-Dastidar, Max Izenberg, Sydne Newberry, Christopher Ferris and Melissa A. Bradley, *Exploring the Civil-Military Divide over Artificial Intelligence*, RAND Corporation, RR-A1498-1, 2022. As of 15 December 2023: https://www.rand.org/pubs/research_reports/RRA1498-1.html

Sanders, Lauren, 'AUKUS is supposed to allow for robust technology sharing. The US will need to Change Its Onerous Laws First', *The Conversation*, 13 July 2023.

Scharre, Paul, *Four Battlegrounds: Power in the Age of Artificial Intelligence*, W.W. Norton & Company, 2023.

Sevastopulo, Demetri, 'UK and Australia Urge Washington to Ease Secrecy Rules in Security Pact', *Financial Times*, 5 March 2023.

Torrens, Shannon, *War Crimes in Afghanistan: The Brereton Report and the Office of the Special Investigator*, Parliament of Australia, undated.

Townshend, Ashley, 'The AUKUS Submarine Deal Highlights a Tectonic Shift in the US-Australia Alliance', Carnegie Endowment for International Peace, 27 March 2023.

Thomas-Noone, Brendan, *Ebbing Opportunity: Australia and the US National Technology and Industrial Base*, United States Studies Centre at the University of Sydney, 2019.

Thomas-Noone, Brendan, *Tech Wars: US-China Technology Competition and What It Means for Australia*, United States Studies Centre at the University of Sydney, 2020.

UK Cabinet Office, "Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy," webpage, last updated 2 July 2021. As of 15 December 2023:
https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

UK Ministry of Defence, *Ambitious, Safe, Responsible: Our Approach to the Delivery of AI-Enabled Capability in Defence*, 2022.

UK Ministry of Defence, and Defence Science and Technology Laboratory, 'World First as UK Hosts Inaugural AUKUS AI and Autonomy Trial', press release, 26 May 2023.

United Nations, *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, September 2019.

United Nations, *Lethal Autonomous Weapon Systems*, General Assembly Resolution 78/241, 12 October 2023.

University of Queensland Cyber and AUSCERT, *Joint Submission—Discussion Paper 2023-2030 Australian Cyber Security Strategy*, 12 April 2023.

U.S. Department of Defense, *Review of Legality of Weapons Under International Law,* Department of Defense Instruction 5500.15, 16 October 1974.

U.S. Department of Defense, 'DOD Adopts Ethical Principles for Artificial Intelligence', press release, 24 February 2020.

U.S. Department of Defense, *Implementation of, and Compliance with, Arms Control Agreements*, Department of Defense Directive 2060.01, 23 June 2020.

U.S. Department of Defense, *Autonomy in Weapon Systems*, Department of Defense Directive 3000.09, 25 January 2023.

U.S. Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, 2023.

Van der Schyff, Jason, 'AUKUS Will Redefine Government–Industry Partnerships', *The Strategist*, 21 February 2023.

Verbruggen, Maaike, 'No, Not That Verification: Challenges Posed by Testing, Evaluation, Validation and Verification of Artificial Intelligence in Weapon Systems', in Thomas Reinhold and Niklas Schörnig, eds., *Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm*, Springer, 2022.

Vogel, Dominic, *Future Combat Air System: Too Big to Fail; Differing Perceptions and High Complexity Jeopardise Success of Strategic Armament Project*, German Institute for International and Security Affairs, 2021.

Wezeman, Pieter D., Alexandra Kuimova and Siemon T. Wezeman, 'Trends in International Arms Transfers, 2021', fact sheet, Stockholm International Peace Research Institute, 2022.

White House, *Indo-Pacific Strategy of the United States*, February 2022a.

White House, *National Security Strategy 2022*, October 2022b.

White House, 'Joint Leaders Statement on AUKUS', press release, 13 March 2023.

White House, 'Australia-United States Joint Leaders' Statement—An Alliance for Our Times', press release, 20 May 2023.

Whittle, Richard, *Predator: The Secret Origins of the Drone Revolution*, Macmillan, 2014.

Williams, Mario D., and Phillyp C. Lawson, *Analyzing the Challenges and Obstacles to Developing and Fielding Autonomous and Semi-Autonomous Systems*, thesis, Naval Postgraduate School, 2020.

Wojton, Heather M., Daniel J. Porter and John W. Dennis, *Test and Evaluation of AI-Enabled and Autonomous Systems: A Literature Review*, Institute for Defense Analyses, 2020.

Wyatt, Austin, *The Disruptive Impact of Lethal Autonomous Weapons Systems Diffusion: Modern Melians and the Dawn of Robotic Warriors*, Routledge, 2021.

Yaacob, Abdul Rahman, 'AUKUS Brings More Than Nuclear Submarines to Southeast Asia', East Asia Forum, 15 September 2023.

About the Authors

Austin Wyatt is an associate researcher at RAND Australia. His research focuses on military transformation, remote, and autonomous systems, military applications of AI and regional security. He has a Ph.D. in political science and military innovation.

James Ryseff is a senior technical policy analyst at the RAND Corporation. His work focuses on how technologies and practices, such as artificial intelligence, cloud computing, cybersecurity, agile software methodologies and large-scale data analysis impact policy problems. Ryseff holds an M.S. in security studies.

Elisa Yoshiara is a Ph.D. student in the Research, Analysis, and Design stream at Pardee RAND Graduate School and an assistant policy analyst at RAND. Her research interests include corporate accountability, conflict financing, illicit trade and complex supply chains. Yoshiara has an M.P.P in public policy.

Benjamin Boudreaux is a professor of policy analysis at the Pardee RAND Graduate School and a policy researcher at RAND working in the intersection of ethics, emerging technology, and human security. His research focuses on the ethics of artificial intelligence technologies, including issues related to equity, surveillance and military applications of AI. Boudreaux has a Ph.D. in philosophy.

Marigold Black is a researcher at RAND Australia. Her research interests include the parameters of Australian sovereignty and national power, the implications of compatible and incompatible conceptions of sovereignty in the modern strategic landscape, intellectual culture and ethos in the Australian Army, civil-military relations, strategic narratives in times of war and peace, ‘just war’ theory and the use of complex machines in conflict, and faith-based diplomacy in a new strategic order. She holds a Ph.D. in history.

James Black is assistant director of the Defence and Security research group at RAND Europe. Black's research focuses on strategy, policy and decision making amidst uncertainty, complexity and rapid change. He holds a double M.A.-M.Sc. in international security.

AUSTRALIA

As the United States and its close allies, such as the United Kingdom (UK) and Australia, face rising threats from China, a key part of their strategy has been to rely on allies and partners to outpace their competitor. However, operating alongside allies and partners also comes with operational challenges and complexities. The authors investigate the challenges and barriers that could inhibit or prevent the co-development of artificial intelligence (AI) between the United States and its closest allies and partners and make recommendations for overcoming those barriers.

www.rand.org/australia

RR-A3079-1