





Japan's Artificial Intelligence Strategy The challenge for AI collaboration across the Trilateral Security Dialogue (TSD)

Trilateral Security Dialogue Paper Series No. 3

Tokyo

Authors

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

ACKNOWLEDGEMENTS This paper has been produced as a result of collaboration between RMIT University's Sir Lawrence Wackett Defence & Aerospace Centre, the Centre for Cyber Security Research and Innovation (CCSRI), the Research Center for Advanced Science and Technology, University of Tokyo, and the Pacific Forum. This research is supported by the Strategic Policy Grants Program (SPGP), Australian Government Department of Defence. The project team includes Professor Aiden Warren, Professor Charles T. Hunt, Professor Matthew Warren, Dr Adam Bartley, and Mark Manantan.

Table of contents

Executive summary
Page 1

Introduction Page 1

Japan's AI landscape Page 2

AI governance and development
Page 3

Strategic culture Page 5

AI cyber security and interoperability
Page 6

The way forward Page 7

Recommendations Page 8

Endnotes Page 9

EXECUTIVE SUMMARY

≺he Australia-United Kingdom--United States (AUKUS) agreement on strategic technology sharing has triggered a broader discussion on the necessity and ability for like-minded states to engage in deeper trade, military, intelligence, and information sharing for national growth and development, and also regional security. This report, like others in this series,¹ highlights the Trilateral Security Dialogue (TSD) as an important platform to enable this agenda. Japan's technological capabilities, strategic alignment, regional security concerns, and shared values make it a natural partner for Australia and the US in defence technology, particularly in the field of AI. There is also strong enthusiasm within the Japanese government and broader AI expert community to move beyond current project based defence cooperation agreements to bridging priority capability development with collaborative partnerships. AI strategy documents highlight an encouraging alignment in this regard.

In this report, the authors highlight the potential for AI defence cooperation with Japan and the role the Defence Trade Cooperation Treaties (DTCT) can play in improving AI collaboration, particularly in dual-use domains. It brings to the fore the influence of uniquely Japanese cultural elements on civil-military cooperation and the need for cybersecurity assurances following recent high profile cyber intrusions within the Japanese Ministry of Defense. The benefits of sandboxing exercises that consider Japan's particular regulatory landscape are also

discussed, along with the importance of establishing focal points in each country to navigate government bureaucracy. The report also emphasises the importance of interaction between governments and public service, industry, and academia from Australia, Japan, and the US, discussing the potential benefits of such interaction, including overcoming linguistic issues in AI and harmonising ethical frameworks and terminology.

INTRODUCTION

This report examines Japan's AI governance and development to explore opportunities and challenges surrounding innovation, interoperability, and ethical considerations. In doing so, it provides a preliminary assessment of Japan's AI readiness for international collaboration. In brief, the report details the transformative impact of AI, especially its implications for strategic collaboration among the TSD countries.

Supported by the Australian Department of Defence, this report provides the key findings from the third Trilateral AI Experts Group dialogue in Tokyo, Japan, jointly organised by RMIT University, the Research Center for Advanced Science and Technology, University of Tokyo, and the Pacific Forum. The workshop took place in November 2023 consisting of consultations with over 30 stakeholders from defence, diplomatic, policy, private sector, and scholarly communities. The dialogue generated insights into enhancing AI cooperation while also highlighting a range of limitations, particularly in understanding how collaboration might take place given current barriers across policy, legal institutions, and strategic cultures.

The first section provides an overview of the evolving Japanese AI landscape. This is followed by a discussion of Japan's regulatory principles and the advancement of technology development policies in the AI space, evaluating the extent to which strategy frameworks have been addressed either via government implementation or policy. Here, the section examines AI readiness in government as defined by the aspirational goals set out in the various public facing strategy documents at the national level. The third part evaluates the strategic cultural aspects contributing to the slow adjustment to advanced technology collaboration with the West, with specific reference to military and defence cooperation. The fourth section on AI cybersecurity and interoperability, widens the aperture on Japan's defence strategy concerning the development of AI in the context of, and the areas and challenges for, collaboration with the other TSD partners. The final section looks at how the government can move forward with its aspirations and policies, before presenting recommendations for how to enhance AI collaboration among TSD partners, deepen technology transference measures, and how to overcome restrictions around industry and military cooperation.

THE JAPANESE AI LANDSCAPE

Recognising a whole range of perceived gaps across

policy, technical, and legal dimensions, the Japanese government has made modest improvements toward AI development and its integration into security policy. The 2021-24 period has marked a pivotal shift in Japan's strategic outlook, spurred by the recognition of AI's transformative potential in national security and defence, particularly in the context of large language models and machine learning. In 2021, Japan's National Security Strategy emphasised the imperative of harnessing AI to fortify its defence capabilities, citing the need to adapt to evolving security challenges in the "digital age." This policy directive laid the groundwork for subsequent initiatives aimed at leveraging AI technologies to enhance Japan's resilience against emerging threats.²

To operationalise its AI-centric security strategy, Japan has embarked on multifaceted endeavours encompassing research and development, international collaboration, and regulatory frameworks – albeit on the last two points there is still a lot to be done. Notably, however, the government has sought to allocate funding to propel AI innovation within defence establishments and academic institutions.³ Concurrently, collaborative ventures with global partners, particularly in the United States, and more recently Australia in 2024, have facilitated knowledge exchange and the adoption of best practices in AI-enabled defence applications, but again, this is an area that was cited by workshop attendees as needing improvement.⁴

Within the broader strategic framework, the



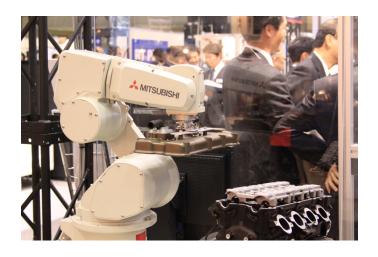
government also maintains that it has prioritised the development of AI-driven platforms for intelligence analysis, cyber defence, and autonomous systems. Investments in advanced AI algorithms and machine learning have bolstered Japan's capacity to process vast volumes of data, enabling an improvement in real-time threat assessment and decision-making.⁵ Furthermore, the integration of AI into cyber defence operations has also improved Japan's ability to pre-empt and mitigate cyber threats, safeguarding critical infrastructure and sensitive information networks, particularly after the failure in 2020 to halt Chinese cyber incursions.⁶

As Japan has navigated the evolving landscape of AI in security, regulatory considerations emerged as a focal point of policy deliberations. The government has implemented measures to ensure the ethical and responsible deployment of AI technologies in defence contexts, emphasising transparency, accountability, and human oversight. Regulatory frameworks delineating the parameters of AI usage in military applications have sought to mitigate risks associated with algorithmic biases, data privacy infringements, and autonomous weapon systems. By fostering a conducive regulatory environment, Japan aims to foster public trust in AI-enabled security initiatives while upholding international norms and standards.

These forward-looking approaches toward AI integration in security policy between 2021 and 2024 reflect an improved and concerted effort to capitalise on technological advancements while addressing associated challenges. However, there are still apparent gaps in the Japanese approach toward AI and, more specifically, its capacity to engage with allies in mitigating such emerging threats. As such, the core driver of this third report correlates to the broader emphasis in examining strategies for enhancing Australia's Artificial Intelligence capability development and defence cooperation between Japan, the United States, and Australia under the TSD framework.

AI GOVERNANCE AND DEVELOPMENT

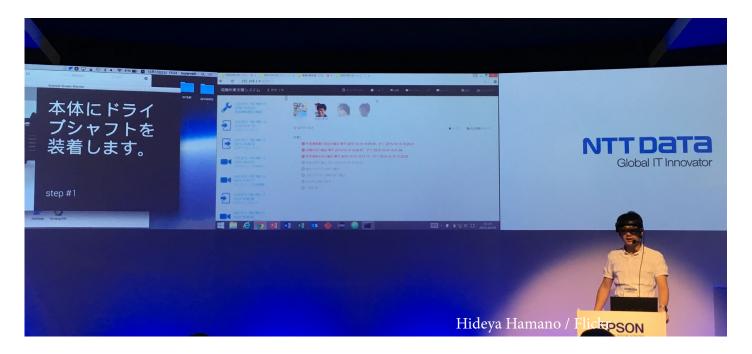
Like Australia and the United States, the development of Japan's national approach to AI has evolved through iterations of documents, white papers, and strategic communications that have crossed between ethical, practical, and more functional proposals for AI adoption. These minor but notable shifts have characterised a unique national AI identity often



at odds with other Western regulatory approaches, making international cooperation challenging. More recently, attention has been paid to international frameworks, prompted by several concerns that Japan's limited international collaboration on AI has reduced its ability to influence international standards. One source of this concern is that Japan's soft law approach to advanced technology development has come into conflict with higher standards in other advanced nations, therefore increasing the reputational risk for Japanese companies looking to engage in global AI markets.

A major concern along this line is that, currently, Japan has no regulations that "generally constrain the use of AI." Explaining this development, Hiroki Habuka notes that "Japan has developed and revised AI-related regulations with the goal of maximizing AI's positive impact on society, rather than suppressing it out of overestimated risks. The emphasis is on a risk-based, agile, and multistakeholder process, rather than a one-size-fits-all obligation or prohibition."10 While there is a growing basis for this line of argument, strong regulatory actions in the EU and the United States have sought to mandate ethical approaches to AI in trade regimes, causing Japanese companies to risk export limitations. According to Hideki Fukawa, director of the defense industry and aerospace division at the Ministry of Economy, Trade, and Industry's (METI), Japanese companies have fallen short of getting certification due to regulatory concerns, even when the product quality has been strong.11

This type of thinking has gradually shifted at the government level as the emphasis on military applications of AI gains traction. The 2023 AI White Paper launched by the ruling Liberal Democratic Party, for instance, has outlined the need to focus more on the



broad-ranging implications of AI across values like human rights and privacy.¹² Meanwhile, Japan's leadership at the 2023 Group of Seven meeting (G7), and specifically the Digital and Tech Ministers' Meeting, has further moved the government to adopt a more agile international framework to "harmonise" regulation and "promote AI governance in a coordinated manner."¹³ This approach, and its associated concerns, have also been raised among leading AI experts and academics in Japan who were consulted to draft a national AI strategy. For now, these discussions are still in the early stages.

This research team's interviews with experts on the sidelines of the workshop highlighted that guidelines had not shifted from AI Governance in Japan Ver. 1.1 report by METI (2021) and its focus on soft law.14 Perhaps more tellingly, neither the Ministry of Foreign Affairs (MOFA) nor the Ministry of Defense (MOD) had formally committed to governance discussions either in Japan or with partners like the European Union or the United Nations. This apparent gap in regulatory requirements and authorities has created uncertainty among businesses, particularly as they aim to broaden international partnerships. Meanwhile, in December 2023, Prime Minister Fumio Kishida announced that the government would establish an AI institute for assessing risks, while also "serving as an accreditation body for AI companies, and participating in international coordination with the United States and the United Kingdom."15 Clearly, an effort is underway to build risk mitigation into the government's AI landscape while incorporating broader adoption.

Traditionally, METI has commanded authority on matters of AI and, subsequently, export licensing, leading to a preference for economic objectives over security concerns.¹⁶ This has reduced the focus on AI collaborative partnerships for defensive applications, but economic considerations are also apparent. According to Rena Sasaki, 95 percent of defence sales among Japanese companies are still in the civilian sector where development prioritisation is still occurring.¹⁷ These numbers demonstrate that the market for AI-enabled defence and associated products remains marginal for companies in Japan, despite the strong international market for the same products. Meanwhile, METI has traditionally sought to focus its role on regulating and controlling sensitive exports than on promoting them; due in part to the long-term ban on weapons exports and defence-related technologies. Prior to 2014, when the ban was lifted, market actors were restricted to the sale of items to the Japanese Self-Defense Forces (JSDF), a condition that contributed to the decline of more than 100 Japanese companies from the market. Over time, innovation in advanced technologies, particularly among smaller firms and startups, was reduced to items that did not intentionally contain military or dual-use applications.

Since 2014, these firms have made a comeback and now promise innovation in various AI domains with military end-use application. However, they continue to face barriers to broader development in international partnerships. One challenge is current export regime controls, and particularly Article 9 of the Japanese constitution which prohibits the export of

95 PERCENT OF DEFENCE SALES AMONG JAPANESE COMPANIES ARE STILL IN THE CIVILIAN SECTOR WHERE DEVELOPMENT PRIORITISATION IS STILL OCURRING. THESE NUMBERS DEMONSTRATE THAT THE MARKET FOR AI-ENABLED DEFENCE AND ASSOCIATED PRODUCTS REMAINS MARGINAL FOR COMPANIES IN JAPAN, DESPITE A STRONG INTERNATIONAL MARKET FOR THE SAME PRODUCTS.

offensive weapons. An outcome of this circumstance is that the defence industry has adopted a passive stance on exports as a default position, and "feels it must wait for the Government of Japan to identify opportunities rather than take the initiative itself." Another challenge is the confusing bureaucracy on AI, with no strong coordination between the departments or government and industry. Major strategy documents like the Defense Technology Strategy (DTS), the Medium to Long-term Technology Outlook (MLTO), and the R&D Vision have called for stronger civil-military fusion, however, guidelines on AI remain less clearly articulated, and the chains of responsibilities for AI as a security enhancing tool remain ambiguous.

These challenges have limited the capabilities of the civilian military industry, which is considered still in its infancy. Enterprises lack "international business acumen to create alliances" with partners for collaboration outside of Japan, noted one major investor, which has and continues to be an inward relationship to the Japanese market.¹⁹ While, as another observer remarked, Japan has "a lot of great talent," it does "not have entrepreneurs in defense right now."²⁰

STRATEGIC CULTURE

One of the major contributing factors to Japan's slow adjustment to military and specifically advanced technology collaboration has been the highly political and sensitive cultural connotations attached to defence cooperation. Traditionally, and still to this day, the relationship between Japanese academia and MOD has been challenged by sensitivities attached to a pacifist constitution, deterring broader cooperation. Even industrial giants, and particularly legacy companies like Mitsubishi Heavy Industries, Kawasaki Heavy Industries Ltd, Toshiba Corporation, and ShinMaywa Industries Ltd have been tepid in their

responses to government outreach, wary of tarnishing their brand among consumers by joining in collaboration with the military.²¹ Notwithstanding this rigidity/inertia, some subtle but significant efforts have been made to develop stronger defence relationships with changes to how AI applications for security are perceived. The government for instance has replaced the term "dual-use" with "multi-use" technologies to imply that more than simply military research is being conducted. MOD has also sought to publicly distance AI dual-use application research between the military and academia by funding projects through a separate agency, the Acquisition, Technology and Logistics Agency (ATLA).

Further linguistic and bureaucratic adjustments have been made to move around the cultural resistance to advanced R&D in AI in the security space. While ATLA has been encouraged to "expand cooperation with other countries in the defense industry field" and develop "Japanese science and technology strengths, and R&D efforts, to meet defense needs," MOD's allocation for R&D continues to sit at around three to four percent of the government's science and technology budget.²² These numbers are small compared to what MOD and ATLA require to establish a Japanese version of America's Defence Advanced Research Projects Agency (DARPA) or Australia's Advanced Strategic Capabilities Accelerator (ASCA). Meanwhile, the focus in the Kishida administration has been on whole-of-government development of AI for economic security. This distinction is important, and while the recent focus on an Economic Security Act positions AI as a strategically important industry to avert national risks and enhance national competitiveness, it also addresses efforts to improve national security. As one workshop participant noted, the



government has specifically avoided the term "military" even as the research is likely to be related or complementary.²³

AI CYBERSECURITY AND INTEROPERABILITY

Under changes to the National Defense Strategy, the Kishida government has unveiled big plans for leveraging cutting-edge technologies like AI for national defence. The announcement in early 2023 to raise defence spending to two percent of GDP by 2027, thereby making it the third-largest defence budget in the world, specifically sought to move the country beyond the "shield and spear" conventional posture with the US providing the bulk of non-nuclear offensive capabilities. In the AI space, this shift in defensive priorities has come with the recognition that MOD and the JSDF will need to significantly embolden the linkages between research results and "development conducted by start-ups and other companies and various research institutions into early production" for national defence.²⁴ According to Shigenori Mishima, vice commissioner and chief technology officer of ATLA, "ATLA will identify technologies that can be directly linked to future warfare," and it will establish an institution that is "best suited to Japan, while referring to good practices as seen in, for example, DARPA and DIU [U.S. Defense Innovation Unit]."25

For Japan, more than Australia and the US, there is a sense of urgency around rebuilding the focus on critical technologies. The penetration by Chinese-linked cyber elements into Japan's defence ministry from 2020 to 2021 damaged Japan's defence industry reputation while reinforcing the notion that the country was not yet ready to join allies in advanced technological collaboration through such arrangements as AUKUS pillar II or the 'Five Eyes' intelligence sharing group. According to the Washington Post, "The hackers had deep, persistent access and appeared to be after anything they could get their hands on - plans, capabilities, assessments of military shortcomings."26 Moreover, the Japanese government's lethargic response to the hack caused allies to rethink their relationship with MOD. US Defense Secretary Lloyd Austin was to remark in public that US-Japan data sharing may need to be slowed until Japanese networks were better secured.²⁷

The response by the Kishida administration was swift. Under the National Security Strategy, National Defense Strategy, and the Defense Build-up Program,



Japan is making various adjustments to the nation's strategic outlook. For instance, military cybersecurity is set to increase four-fold to 4,000 people. In addition to reinforcing efforts in information security and cybersecurity, the Defense Strategy further articulated that the government would pursue means to enhance the US-Japan alliance's technological edge, interoperability, readiness, and persistent warfare capabilities. Moreover, it would focus on "defense equipment and technology cooperation through joint analysis and joint research in cutting-edge technology, joint development and production of defense equipment, improvement in mutual interchangeability, shared use and reinforcement of various networks, expansion of production and maintenance capability of U.S. military equipment in Japan and reinforcement of supply-chain."28 The language in the document represents a major shift from previous policies and actions, as demonstrated by the former reluctance of MOD to allow US cyber specialists to analyse the Chinese hack from Japanese systems.29 The defence strategy, along the with the DTS, the MLTO, and the R&D Vision have sought to alleviate these cyber concerns and rebuild trust between Japan and its allies.

As a result, but particularly more recently, both the US and Australia have made agreements with Japan in building collaborative AI. With the US, Japan announced an agreement in December 2023 to

FOR JAPAN, MORE THAN AUSTRALIA OR THE US, THERE IS A SENSE OF URGENCY AROUDN REBUILDING THE FOCUS ON CRITICAL TECHNOLOGIES.

research AI for uninhabited aerial vehicles (UAV) for future employment with next generation aircraft.³⁰ Meanwhile, Australia and Japan signed an agreement in January 2024 to enhance strategic capabilities in robotic and autonomous systems for undersea warfare. The project will be hosted between ATLA and Australia's Defence Science and Technology Group and is the first arrangement under the bilateral research, development, test and evaluation (RDT&E) arrangement signed in June 2023.³¹ For Australia in particular, the National Defense Strategy illustrates that Japanese military policymakers and analysts perceive the defence relationship with Australia as being fundamental to building regional and integrated deterrence.

In addition to bolstering relations with the United States, Tokyo seeks to deepen the "Special Strategic Partnership" with Australia at all levels including the "Foreign and Defense Ministerial Consultations ("2+2"), bilateral/multilateral training and exercises, [and] defense equipment and technology cooperation." In short, Japan seeks to "build the closest cooperative relationship second only to the Japan-U.S. defense cooperation." These statements, taken also within the context of the agreements mentioned above, are likely to go far in harmonising technology networks and information and data streams between the three member countries of the TSD.³² So far, these efforts have been bilateral, but with further integration, the logical next step is to branch out to the trilateral agreement.

THE WAY FORWARD

Japan's new National Defense Strategy, along with commitments to Australia and the United States, illustrates that existing recruitment problems are likely to endure. One estimate by METI, for instance, suggests that Japan will face a shortfall of 789,000 software engineers by 2030. While this will have an impact on economic productivity, the implications for defence are also concerning. The JSDF have not met a recruitment target since 2013, and the current attrition rate is considered high. Meanwhile, both MOD and the JSDF must compete with the private sector for new recruits, which generally offers better employment packages, and does not come with the stigma of being seen as pro-military.³³

Japan's shrinking population, and its shortage of personnel working in advanced systems, means that

AI will become central to future defence applications. Autonomous and AI-enabled systems will be required, for instance, to defend against cyber and electronic warfare attacks. As cyber threat vectors are projected to outpace human capabilities, systems that can act increasingly without human intervention will be at an enormous advantage.

For Japan, channelling into this capability would ensure interoperability with US (and in the future Australian) forces. However, as noted recently by RAND Corporation, "the United States will be able to integrate its networks with Japan's only if it has confidence that doing so would not lead to backdoor infiltration of its own networks."³⁴ This implies that the road is likely to be a long one, and there are already concerns that Japan's transition may be too slow to affect the balance of power in the region, and contribute to broader deterrence against China.³⁵

For now, Japan is playing catch up in the cyber domain, and lacks sufficient implementation and interface in other key domains. According to the IMD World Digital Competitiveness Ranking, Japan currently sits at 28 out of 63 countries on technical knowledge.³⁶ Meanwhile, the Australian Strategic Policy Institute's Tech Tracker has Japan trailing behind on AI capabilities. For instance, for research contribution in the field, Japan scores 15th (0.9% proportion of top 10% publications) for research on adversarial AI, 20th in terms of AI algorithms and hardware accelerators, 11th for machine learning, and 11th (in countries ranked highest in H-index) for natural language processing. These measures are not definitive, and there are others that Japan excels at. But they do illustrate a shortfall in defence-related AI and cyber capabilities that will need to be addressed. All three TSD states face AI-related skills shortages, particularly in the government and defence sectors. And no one state has been able to dominate all fields of AI.

Finally, data linking and harmonisation among international partners will in the long run work toward an advantage for machine learning and Large Language Models. Among the TSD partners, however, Japan has much to catch up on.

RECOMMENDATIONS

The following recommendations offer ways to maximise the potential of the TSD for AI defence cooperation.

- 1. Encourage the establishment of a Defence Trade Cooperation Treaty (DTCT) between all three TSD members, akin to the US-Australian DTCT, would improve AI collaboration, particularly in dual-use domains where Japan has considerable expertise. A DTCT would speed up tech transfer and knowledge acquisition between the partners, boost interoperability among teams and defence forces, reduce export control barriers, facilitate new defence technology cooperation, including codevelopment, while also fostering mutual trust and information and data sharing. This step is necessary for transforming TSD AI collaboration beyond the current framework, and will go far in creating a community of DTCT companies within a common market, such as the US-Australian-UK one already in place.³⁷ Such an arrangement has further implications for AUKUS pillar II and the deepening of advance technology cooperation among likeminded allies.
- 2. Recognise and develop cooperation with Japan that considers strong cultural elements which continue to influence civil-military cooperation on advanced technologies. Australia, with the US, can incorporate changes to how agreements and even dialogues are framed, for instance, by minimising language that contradicts the position of Article 9 of Japan's constitution, while also pursuing a strong ethical basis of use.
- 3. Consider a cyber partnership for responding to international cyber intrusions. Japan has made excellent progress since the 2020-2021 Chinese cyber intrusions; however, assurances must be made before new arrangements are inked. This could be in the form of a cyber partnership for responding to international cyber intrusions. Building trust on cyber defences for enhancing protections of intelligence and data networks will do much to ensure bilateral and trilateral AI partnerships can reach their full potential. This will require first and foremost more interaction between cyber units of each country, followed by a harmonisation of processes in how to respond to threats and cyber penetration.
- **4. Develop exercises between TSD members that model future advanced technology cooperation using sandboxes.** Such exercises will help to bring Japan's unique regulatory landscape into focus and promote further integration of AI systems and processes. Because there are separate and often confusing authorities for AI in Japan, navigating government bureaucracy will require a point person from each country to expedite applications for collaboration. This will be required for government and Defence as much as for industry. For Japan's burgeoning AI industry, these links will be crucial to breaking out from a formerly closed market (and for Australian Defence industry actors looking to enter the Japanese market) and contribute to a more advanced form of integrated deterrence.
- 5. Establish a mechanism / platform for higher tempo AI work teams from Australia, Japan, and the US. Whether belonging to ASCA, DARPA or government, further interaction between representatives of TSD member states will be instrumental in overcoming linguistic issues in AI, particularly around questions of ethics. Enhanced collaboration can lead to a deeper understanding and harmonisation of ethical frameworks and terminology, which is crucial for the development of AI systems that align with shared ethical principles.
- 6. Develop working groups involving AI experts, ethicists, and policymakers from all three countries. This platform can facilitate regular exchanges, discussions, and joint research projects focused on ethical considerations in AI development and deployment. These workshops will help to develop a shared ethical framework that outlines the major issues around soft and hard regulations for AI and defence.

- 7. Foster linguistic understanding by promoting language exchange programs, joint research projects, and collaborations between linguists and AI researchers. This will help in developing AI systems that can better understand and interpret language nuances across different languages and cultures.
- 8. Strengthen collaboration on data sharing practices that ensure the ethical collection, use, and sharing of data for AI development. Develop guidelines for data sharing that prioritize privacy, consent, and security, and promote responsible data stewardship.

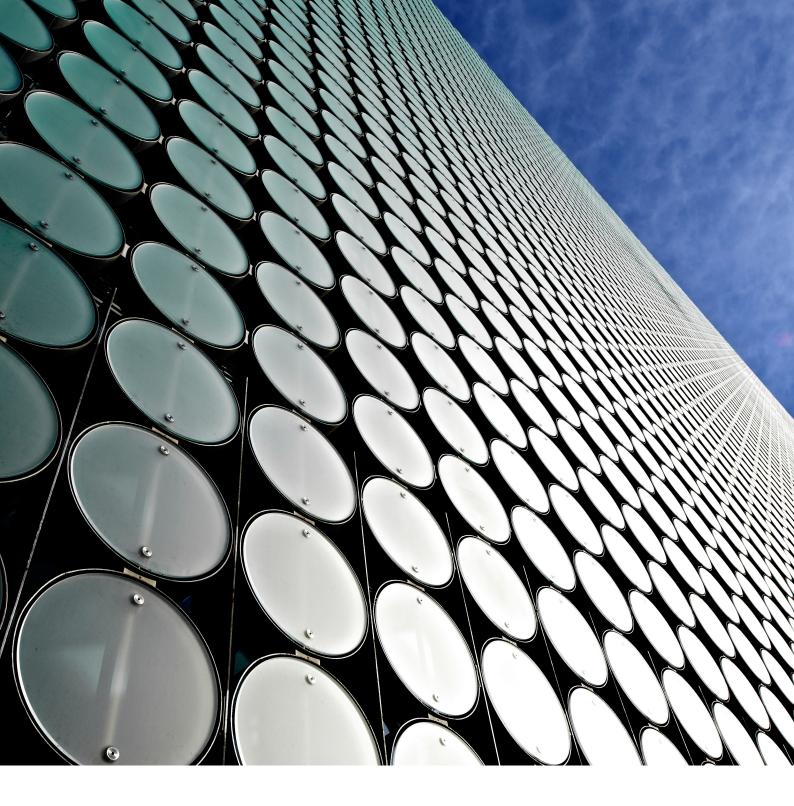
ENDNOTES

- 1. Warren, A., Hunt, C., Warren, M., Bartley, A., & Manantan, M. (2023). Trilateral Security Dialogue Paper Series No. 1 (Washington D.C.) Australia In: Australia Department of Defence Melbourne; https://www.internationalaffairs.org. au/publication/the-trilateral-security-dialogue-defence-cooperation-artificial-intelligence/; Warren, A., Hunt, C., Warren, M., Bartley, A., & Manantan, M. (2023). Trilateral Security Dialogue PaperSeriesNo.2(Melbourne) Australia In: Australia Department of Defence Melbourne, https://www.rmit.edu.au/research/centres-collaborations/cyber-security-research-innovation/australia-artificial-intelligence-strategy
- 2. Ministry of Foreign Affairs of Japan. (2021) "National Security Strategy of Japan," December.
- 3. Ministry of Defense of Japan. (2021). "Defense of Japan 2021," September.
- 4. Japan Ministry of Defense. (2022) "Japan-U.S. Joint Statement on Defense Cooperation," April.
- 5. Japan Ministry of Defense. (2023) "Interim Report on Defense of Japan 2023," June.
- 6. Cabinet Secretariat of Japan, (2022). "Cybersecurity Strategy," February.
- 7. Ministry of Economy, Trade and Industry of Japan. (2022) "Artificial Intelligence Technology Strategy," July.
- 8. Ministry of Defense of Japan. (2024) "Guidelines for the Use of AI in Defense Applications," January.
- 9. Ministry of Internal Affairs and Communications of Japan, (2023) March.
- 10. Hiroki Habuka. (2023). Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency. Center for Strategic and International Studies Report, February 14. Access here https://www.csis.org/analysis/japans-approach-airegulation-and-its-impact-2023-g7-presidency
- 11. Stew Magnuson. (2023). Japan Pushing its Tech Companies to Partner with U.S. Defense Industry.

- National Defense, February 6. Accessed via https://www.nationaldefensemagazine.org/articles/2023/6/2/japan-pushing-its-tech-companies-to-partner-with-us-defense-industry
- 12. The AI White Paper: Japan's National Strategy in the New Era of AI. (2023). LDP Headquarters for the Promotion of Digital Society Project Team on the Evolution and Implementation of AI. Accessed via https://www.taira-m.jp/ldp%E2%80%99s%20 ai%20whitepaper_etrans_2304.pdf
- 13. Arisa Ema, Tagui Ichikawa, Toshiya Jitsuzumi, Hiroshi Nakagawa, Hiroki Habuka, and Yuko Harayama. (2023). International Collaboration in AI Governance: Key Considerations for the Council of Europe's AI Convention and Japan's Response. Institute for Future Initiatives Policy Recommendation No. 25. Accessed via https://ifi.u-tokyo.ac.jp/en/wp-content/uploads/2023/10/policy_recommendation_tg_20231031e.pdf
- 14. AI Governance in Japan Ver. 1.1 (2021). Report from the Expert Group on How AI Principles Should be Implemented. Ministry of Economy, Trade, and Industry. July 9. Access here https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf
- 15. Japan to Establish AI Safety Institute in January 2024. Digwatch, 21 December 2023. Accessed via https://dig.watch/updates/japan-to-establish-ai-safety-institute-in-january-2024
- 16. Tamoo Marukawa. (2013). Japan's High-Technology Trade with China and Its Export Control. Journal of East Asian Studies 13, No. 3: pp 483-501.
- 17. RenaSasaki.(2022).JapanNeedsaDefenseIndustrial Revolution. Foreign Policy, March 9. Accessed via https://foreignpolicy.com/2023/03/09/japan-defense-industrial-revolution-security/
- 18. Michael Hadlow and Crystal Pryor. (2018). Japan's Defense Exports: "Three Years of Sitting

- on a Stone". Issues and Insights working paper Vol. 18, Pacific Forum. Accessed via https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/PacificForum_Japan%20Defense%20Exports.pdf
- 19. Magnuson. (2023). Japan Pushing its Tech Companies to Partner with U.S. Defense Industry.
- 20. Mashiro Okoshi. (2023). U.S. Venture Capital Firm VC Targets Japan's Defense Industry. Nikkei Asia, September 28. Accessed via https://asia.nikkei.com/Business/Aerospace-Defense-Industries/U.S.-venture-capital-firm-8VC-targets-Japan-s-defense-industry
- 21. Henry Ridgewell. (2023). Japan Struggles to Booste Defense Industry Amid China's Military Ambitions. VOA News, August 10. Accessed via https://www.voanews.com/a/japan-struggles-to-boost-defense-industry-amid-china-s-military-ambitions/7219689.html
- 22. Key note address by Dr. Shigenori Mishima, vice commissioner and chief technology officer of Japan's Acquisition, Technology & Logistics Agency (ATLA) on Japan's Defence Technology Strategy, Indo-Pacific Defense Forum, December 18, 2023, accessed via https://ipdefenseforum.com/2023/12/japans-defense-technology-strategy/
- 23. Workshop participant, November 8, 2023, Tokyo.
- 24. National Defense Strategy, Ministry of Defense, Japan, December 16, 2022, p. 16. Accessed via https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf
- 25. Key note address by Dr. Shigenori Mishima.
- 26. Ellen Nakashima. (2023). "China Hacked Japan's Sensitive Defense Networks, Officials Say." *The Washington Post*, 8 August. Accessed via https://www.washingtonpost. com/national-security/2023/08/07/china-japan-hack-pentagon/
- 27. Ibid.
- 28. National Defense Strategy, Ministry of Defense, Japan, December 16, 2022, p. 20. Accessed via https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf
- 29. Nakashima. (2023). "China Hacked Japan's Sensitive Defense Networks, Officials Say."
- 30. Japan and U.S. Agree on AI Research for Drones to Assist New Fighter Jet. (2024). *The Japan Times*, 28 January. Accessed via https://www.japantimes.co.jp/news/2024/01/28/japan/politics/japan-us-ai-research-for-drones/
- 31. Australia and Japan Sign Research Agreement

- for Undersea Warfare. Australian Government Department of Defence, 23 January 2024. Accessed via https://www.defence.gov.au/news-events/releases/2024-01-23/australia-and-japan-sign-research-agreement-undersea-warfare
- 32. National Defense Strategy, Ministry of Defense, Japan, December 16, 2022. Accessed via https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf
- 33. The SDF Has a Big Problem: Filling its Ranks. (2023). *Japan Times*, 3 November. Accessed via https://www.japantimes.co.jp/editorials/2023/11/03/sdf-recruitment/
- 34. Hornung, Jeffrey W., Scott Savitz, Jonathan Balk, Samantha McBirney, Liam McLane, and Victoria M. Smith, Preparing Japan's Multi-Domain Defense Force for the Future Battlespace Using Emerging Technologies. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/perspectives/PEA1157-1.html.
- 35. Jennifer Kavanagh. (2023). Japan's New Defence Budget is Still Not Enough." Carnegie Endowment for International Peace, Commentary, 8 February. Accessed via https://carnegieendowment. org/2023/02/08/japan-s-new-defense-budget-is-still-not-enough-pub-88981
- 36. World Digital Competitiveness Ranking. (2023). International Institute for Managing Development. Accessed via https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/
- 37. Arthur Herman. (2016). The Awakening Giant: Risks and Opportunities for Japan's New Defense Export Policy. Hudson Institute report, December 19. Accessed via https://www.hudson.org/national-security-defense/the-awakening-giant-risks-and-opportunities-for-japan-s-new-defense-export-policy



www.rmit.edu.au



