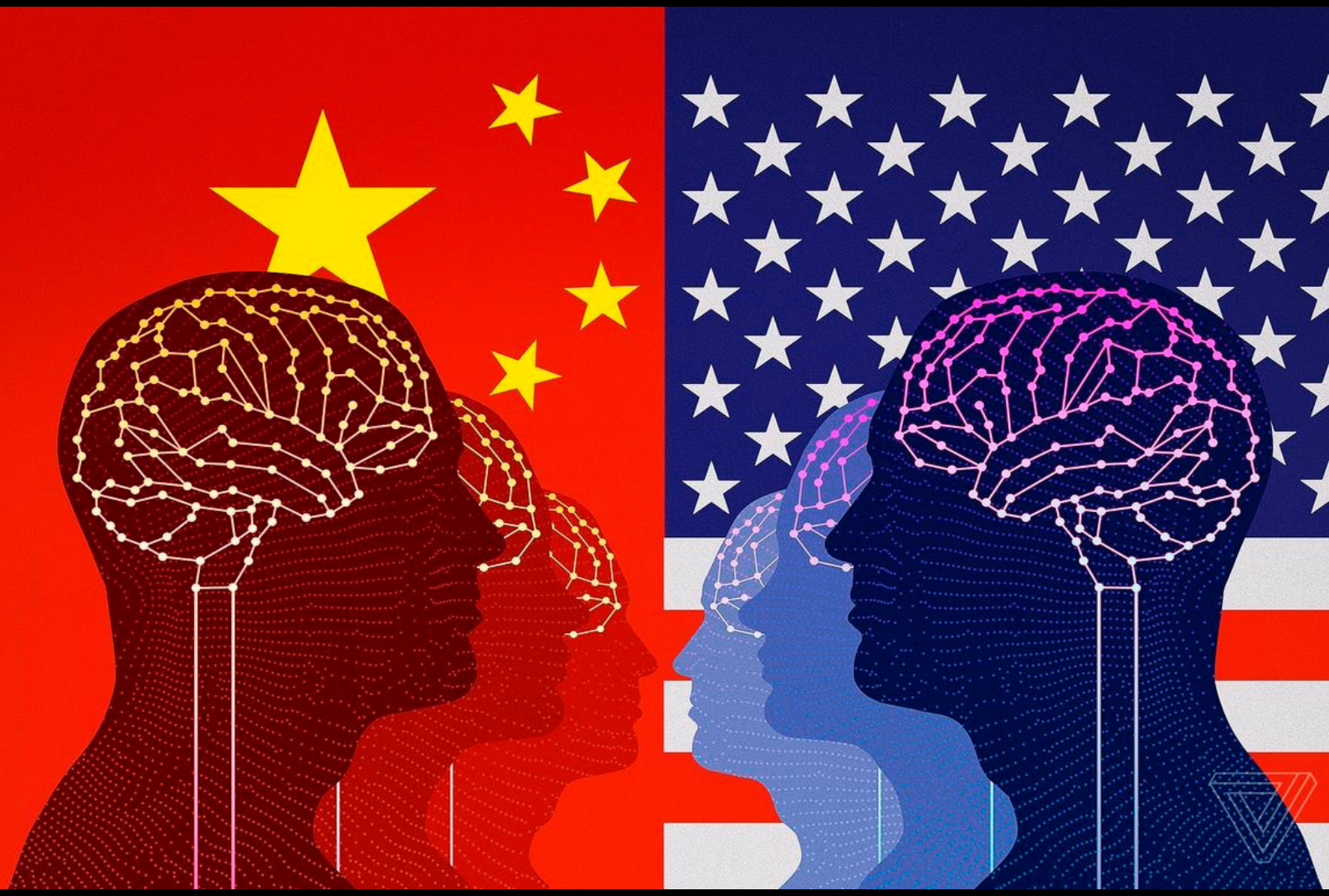
Technological entanglement

Cooperation, competition and the dual-use dilemma in artificial intelligence

Elsa B. Kania



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No.7/2018

About the author

Elsa B. Kania an Adjunct Fellow with the Center for a New American Security's Technology and National Security Program. She focuses on Chinese defense innovation in emerging technologies in support of the Artificial Intelligence and Global Security Initiative at CNAS, where she also acts as a member of the research team for the new Task Force on Artificial Intelligence and National Security. Her research interests include Chinese military modernization, information warfare, and defense science and technology. Elsa is an independent analyst, consultant, and co-founder of the China Cyber and Intelligence Studies Institute (CCISI). She was also a 2018 Fulbright Specialist with the Australian Strategic Policy Institute's International Cyber Policy Centre. Elsa works in support of the China Aerospace Studies Institute (CASI) through its Associates Program, and she is a consulting analyst with Pointe Bello and a policy advisor for the non-profit Technology for Global Security. Elsa has been named an official "Mad Scientist" by the U.S. Army's Training and Doctrine Command.

Elsa is a graduate of Harvard College (summa cum laude, Phi Beta Kappa), where her thesis on the evolution of the PLA's strategic thinking on information warfare was awarded the James Gordon Bennett Prize. Her prior professional experience includes time with the Department of Defense, the Long Term Strategy Group, FireEye, Inc., and the Carnegie-Tsinghua Center for Global Policy. While at Harvard, she worked as a research assistant at the Belfer Center for Science and International Affairs and the Weatherhead Center for International Affairs. Elsa was a Boren Scholar in Beijing, China, and she is fluent in Mandarin Chinese.

What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

Important disclaimer

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home

First published June 2018.

Cover image: Illustration by James Bareham, Creative Director at *The Verge* in the article China and the US are battling to become the world's first AI superpower published 3 August 2017. ASPI ICPC has attained a non-exclusive grant to use this image for this report. This image cannot be re-published unless permission is granted by Vox Media Inc.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Technological entanglement

Cooperation, competition and the dual-use dilemma in artificial intelligence

Elsa B. Kania

Policy Brief
Report No.7/2018

Contents

What's the problem?

Despite frequent allusions to a race—or even an 'arms race'—in artificial intelligence (AI), US leadership and China's rapid emergence as an AI powerhouse also reflect the reality of cooperation and engagement that extend across the boundaries of strategic competition.[1] Even as China and the US, the world's emergent 'AI superpowers',[2] are increasingly competing in AI at the national level, their business, technology and research sectors are also deeply 'entangled' through a range of linkages and collaborations. That dynamic stems from and reflects the nature of AI research and commercialization—despite active competition, it is open and often quite collaborative.[3] These engagements can, of course, be mutually beneficial, but they can also be exploited through licit and illicit means to further China's indigenous innovation and provide an asymmetric advantage.[4] The core dilemma is that the Chinese party-state has demonstrated the capacity and intention to co-opt private tech companies and academic research to advance national and defence objectives in ways that are far from transparent.

This has resulted in a 'dual-use dilemma' in which the openness that's characteristic of science and innovation in democracies can result in unforeseen consequences, undermining the values, interests and competitiveness of the US, Australia and other like-minded nations in these strategic technologies.[5] These 'entanglements' have included ties between US tech firms and Chinese partners with military connections,[6] as well as cooperation between Australian universities and the Chinese People's Liberation Army (PLA).[7] Despite the genuine advantages they may offer, such problematic partnerships can also result in the transfer of dual-use research and technologies that advance Chinese military modernisation, perhaps disrupting the future balance of power in the Indo-Pacific, or facilitate the party-state's construction of surveillance capabilities that are starting to diffuse globally. These adverse externalities have troubling implications for US military advantage, authoritarian regime resilience and even the future of democracy.[8] How should policymakers balance the risks and benefits of such entanglement,[9] while enhancing competitiveness in this strategic technology?

What's the solution?

These unique and complex dynamics require a range of policy responses that balance the risks and benefits of these partnerships, collaborations and engagements. To enhance situational awareness, policymakers should examine closely research, academic and commercial partnerships that may prove problematic, and then consider updates and revisions to national export controls, defence trade controls and investment review mechanisms as targeted countermeasures. While there is a rationale for visa screening of foreign nationals who plan to study or research sensitive technologies, restrictions should be imposed only on the basis of evidence of direct and clear connections to foreign militaries, governments or intelligence services,[10] and scrutiny should focus more on organisations engaging in talent recruitment that are linked to the Chinese central and local governments or to the Chinese Communist Party (CCP). At the same time, there are compelling reasons to sustain scientific cooperation, with safeguards for risk mitigation, including transparency and the protection of sensitive data.

Critically, the US and Australia must pursue policies that actively enhance the dynamism of their own innovation ecosystems to ensure future competitiveness. It is vital to bolster declining support for science and commit to increasing funding for basic research and the long-term development of strategic technologies. Given the criticality of human capital, governments should prioritise improving the accessibility and affordability of STEM education at all levels, while attracting and welcoming talent through favourable immigration policies. In this quest for competitive advantage, the US and Australia must also pursue closer public–private partnerships and expand alliance cooperation on defence innovation.

AI 'without borders'

Today, national competition in AI is intensifying at a time when the engine for technological innovation in such dual-use technologies has shifted from governments to commercial enterprises. In today's complex, globalised world, flows of talent, capital and technologies are rapid, dynamic and not readily constrained by borders. Chinese investments and acquisitions in Silicon Valley—and US investments in China—are sizable and increasing, despite intense concerns about the security risks of such investments,[11] which have motivated reforms to the Committee on Foreign Investment in the United States (CFIUS) and could result in discretionary implementation of China's national security review mechanism in response.[12] This increased globalisation of innovation ecosystems has proven beneficial to AI development, and dynamic US and Chinese companies are emerging as world leaders in the field.

Increasingly, these enterprises are quite international in their outlook, presence and workforce while engaging in a global quest for talent.[13] For the time being, the US remains the centre of gravity for the top talent in AI, and Silicon Valley is the epicentre of this talent 'arms race'.[14] While currently confronting major bottlenecks in human capital, China has great potential, given the number of graduates in science and engineering and the range of new training and educational programs dedicated to cultivating AI talent.[15] At the same time, the Chinese government is actively incentivising the return and recruitment of 'strategic scientists' via state talent plans.[16] At the forefront of the AI revolution, Baidu and Google epitomise in their strategic decisions and activities the linkages and interconnectivity among such global centres of innovation as Silicon Valley and Beijing.[17]

Baidu has prioritised AI and has emerged as a leading player in this domain. It created the Institute for Deep Learning in Beijing in 2013 and then established its Silicon Valley Artificial Intelligence Laboratory (SVAIL), which employs about 200 people, in 2014.[18] Baidu's CEO, Li Yanhong (李彦宏, or Robin Li), advocated as early as 2015, prior to the Chinese Government's decision to prioritise AI, for a 'China Brain' plan that would involve a massive national initiative in AI, including welcoming military funding and involvement.[19] Increasingly, Baidu has actively invested in and acquired US AI start-ups, including xPerception and Kitt.ai,[20] while seeking to expand its US-based workforce. The company has stated that Silicon Valley 'is becoming increasingly important in Baidu's global strategy as a base for attracting world-class talent.'[21] In March 2017, Baidu announced plans to establish a second laboratory in Silicon Valley, which is expected to add another 150 employees.[22] Notably, Baidu has also launched the Apollo project, which is a collaborative initiative to advance the development of self-driving cars that involves more than 100 tech companies and automakers, including Ford, NVIDIA, and Microsoft.[23] At the same time, Baidu is engaged in research on military applications of AI, particularly command and control.[24]

Google remains at the forefront of AI development, leveraging an international presence and global workforce. Beyond Silicon Valley, Google has opened AI research centres in Paris, New York and Tokyo,[25] and it will soon add Beijing and then Accra, Ghana.[26] When Google announced the opening of the Google AI China Center in March 2017, chief scientist Fei-Fei Li declared, 'I believe AI and its benefits have no borders. Whether a breakthrough occurs in Silicon Valley, Beijing, or anywhere else, it has the potential to make everyone's life better for the entire world.'[27] She emphasised, 'we want to work with the best AI talent, wherever that talent is, to achieve' Google's mission.[28] Google's decision to expand its presence and activities in China, after withdrawing its search product from the market due to concerns over censorship, surveillance and the theft of intellectual property via cyber espionage in 2010,[29] reflects this enthusiasm for the potential of future talent in China—and probably the availability of a sizable market and massive amounts of data as well.[30] At the same time, this decision presents an interesting counterpoint to Google's recent issuing of a statement of principles that included a commitment not to build technologies used for surveillance.[31] Given the dual-use nature of these technologies, Google's choice to engage in China may involve risks and raise ethical concerns,[32] especially considering the Chinese party-state's agenda for and approach to AI.

China's global AI strategy and ambitions

At the highest levels, the Chinese Government is prioritising and directing strong state support to AI development, leveraging and harnessing the dynamism of tech companies that are at the forefront of China's AI revolution. The New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划), released in July 2017, recognised this strategic technology as a 'new focal point of international competition', declaring China's intention to emerge as the world's 'premier AI innovation centre' by 2030.[33] The Three-Year Action Plan to Promote the Development of New-Generation Artificial Intelligence Industry (促进新一代人工智能产业发展三年行动计划) (2018–2020), released in December 2017, called for China to achieve 'major breakthroughs in a series of landmark AI products' and 'establish international competitive advantage' by 2020.[34] China's central and local governments are providing high and ever-rising levels of funding for research and development on next-generation AI technologies, while seeking to create a robust foundation for innovation by introducing new talent and education initiatives, developing standards and regulatory frameworks, and supporting the availability of data, testing and cloud platforms.[35]

China's ambition to 'lead the world' in AI is self-evident.[36] These plans and policies should be contextualised by its tradition of techno-nationalism and current aspirations to emerge as a 'science and technology superpower' (科技强国).[37] In recent history, indigenous Chinese innovations, particularly defence technological developments, have been advanced and accelerated through licit and illicit means of tech transfer, including extensive industrial espionage.[38] However, pursuing a new strategy of innovation-driven development,[39] China is actively seeking to progress beyond more absorptive approaches to innovation and instead become a pioneer in emerging technologies, including through increasing investment in basic research.[40] To further this agenda, the Chinese government is avidly targeting overseas students and scientists, offering considerable incentives via talent plans and engaging in recruitment via 'talent bases' and organisations that are often linked to the CCP or to central or local governments.[41] [42]

At this point, the success of these initiatives remains to be seen, and there are even reasons to question whether an AI bubble may arise due to excessive enthusiasm and investments. Although China's future potential for innovation shouldn't be dismissed or discounted, this 'rise' in AI often generates alarm and exuberance that can distract from recognition of major obstacles that remain. As its plans openly admit, China continues to lag behind the US in cutting-edge research and is attempting to compensate for current shortfalls in human capital.[43] Notably, China confronts continued difficulties in the development of indigenous semiconductors,[44] which will be critical to the hardware dimension of future advances in AI,[45] despite billions in investment and quite flagrant attempts to steal intellectual property from US companies.[46]

While gradually becoming more capable of truly independent innovation, China also intends to coordinate and optimise its use of both domestic and international 'innovation resources'.[47] Notably, the New Generation AI Development Plan calls for an approach of 'going out' (走出去) involving overseas mergers and acquisitions, equity investments and venture capital, along with the establishment of R&D centres abroad.[48] For instance, a subsidiary of the China Electronics Technology Group Corporation (CETC), a state-owned defence conglomerate, established an 'innovation centre' in Silicon Valley in 2014, which seeks to take advantage of that ecosystem with a focus on big data and other advanced information technologies.[49] In Australia,[50] CETC established a joint research centre with the University of Technology Sydney (UTS), which will focus on AI, autonomous systems and quantum computing, in April 2017.[51] Starting in 2018, CETC's Information Science Academy is also funding a project at UTS on 'A Complex Data Condition Based Public Security Online Video Retrieval System', which could have clear applications in surveillance.[52] There have been extensive collaborations on dual-use AI technologies between PLA researchers from the National University of Defence Technology and academics at UTS, the University of New South Wales and the Australian National University.[53] Meanwhile, Huawei is actively funding research and pursuing academic partnerships in the US and Australia, including through its Huawei Innovation Research Program.[54] China's 'One Belt, One Road' strategy is also concentrating on scientific and technological cooperation, including educational exchanges and research partnerships, such as a new Sino-German joint AI laboratory.[55] Some of these new collaborations will focus on robotics and AI technologies, often enabling access to new sources of data that may facilitate China's emergence as a global leader in AI development.[56] In certain instances, China's provision of funding to these initiatives may also reorient the direction of research based on its own priorities.[57]

As China seeks to advance indigenous innovation, the strategy of 'going out' is complemented by a focus on 'bringing in' (引进来) to ensure that vital talent and technologies are drawn back into China.[58] At the same time, the Chinese government is evidently seeking to ensure that innovation 'made in China' will stay in China. As the US undertakes reforms to CFIUS, China could respond by recalibrating the implementation of its own national security review process, which is ambiguous enough to allow for great discretion in its application, pursuant to an expansive concept of national or state security (国家安全).[59] Notably, the State Council has also issued a new notice that requires that scientific data generated within China be submitted to state data centres for review and approval before publication.[60] The policy purports to promote open access to and sharing of scientific data within China, while creating ambiguous new restrictions that, depending upon their implementation, could render future cooperation asymmetrical in its benefits.[61] Given these factors, while opportunities for research cooperation should often be welcomed, it is also important to ensure transparency regarding the research and intellectual property that may result from it, as well as the security of valuable or sensitive datasets.

China's integrated approach to indigenous innovation

In pursuit of its dreams of AI dominance, China is pioneering a new paradigm of indigenous innovation that takes advantage of critical synergies through creating mechanisms for deeper integration among the party-state, technology companies and the military. The CCP seeks not only to support private Chinese companies in their quest for innovation but also to control and guide them, ensuring that the companies serve the needs of the party and don't become a threat to it. China's 'champions' in AI—Baidu, Alibaba, Tencent and iFlytek—are at the forefront of innovation in the field, and this 'national team' will be supported and leveraged to advance state objectives and national competitiveness.[62] For instance, Baidu is leading China's National Engineering Laboratory for Deep Learning Technologies and Applications (深度学习技术及应用国家工程实验室),[63] and iFlytek is leading the State Key Laboratory of Cognitive Intelligence (认知智能国家重点实验室).[64] It seems likely that the research in these new laboratories will be directed to dual-use purposes. These champions will also undertake the development of new open innovation platforms in AI: Baidu will be responsible for autonomous vehicles, Alibaba Cloud (Aliyun) for smart cities, Tencent for medical imaging and iFlytek for smart voice (e.g., speech recognition, natural-language processing, machine translation, etc.).[65] The platforms will be piloted in the Xiong'an New Area, a development southwest of Beijing that's intended to be a futuristic demonstration of Chinese innovation and to showcase AI technologies and applications in action.[66]

Meanwhile, Xi Jinping has recently reaffirmed the Mao-era sentiment that 'the party leads everything', and China's advances in AI must also be understood in the context of this system, in which the CCP is steadily increasing its control over private companies.[67] In recent years, the CCP has introduced representatives of party branches and committees into notionally private companies,[68] which have started to undertake more active 'party building' (党建) activities that are intended to expand the CCP's presence and influence.[69] Just about every major tech company, including Baidu, Alibaba, Tencent, Sohu, Sina and NetEase, has a party secretary, who is often a fairly senior figure within the company, and new requirements may even require all listed companies to 'beef up party building'.[70] For example, in March 2017, the CCP Capital Internet Association Commission (中共首都互联网协会委员会) convened a party committee expansion meeting and a work meeting on grassroots party building that brought together the leaders of many prominent companies.[71] At the meeting, Baidu Party Secretary Zhu Guang (朱光), who is also a Senior Vice President responsible for public relations and government affairs,[72] talked about innovation in 'party building work', including the development of a mobile solution for 'party building'. He committed Baidu to leveraging its capabilities in big data and AI applications, as well as its 'ecological advantage', to enhance the effectiveness of such efforts.[73] This blurring of the boundaries between the party-state and its champions may create a tension between national strategic objectives and these companies' global commercial interests.[74] Increasingly, the CCP is even attempting to extend its reach into, and authority over, foreign companies operating in China.[75]

The dual-use dilemma in China's AI development

The future trajectory of AI in China will inherently be shaped and constrained by the interests and imperatives of the party-state, and international collaboration with Chinese research institutions and corporate actors needs to be understood, and engaged in, with this important context in mind. Critically, AI will enhance both economic development and military modernization, while reinforcing the party's ability to control its population through domestic surveillance, all of which are integral to the regime's security and legitimacy. China's AI plans and policies include the concern that AI will remain 'secure and controllable' (安全 , 可控), given the risks of societal disruption, while highlighting the importance of AI 'to elevate significantly the capability and level of social governance, playing an irreplaceable role in effectively maintaining social stability', thus bolstering regime security.[76] Indeed, the pursuit of such 'innovations' in social governance through big data and AI has included the construction of predictive policing and surveillance capabilities, often developed with the assistance of start-ups such as SenseTime and Yitu Tech, that have often been abused, particularly in Xinjiang.[77] Given the party's attempts to extend its reach—and the trend towards deeper integration in civilian and military AI efforts in China—it can be difficult to disentangle notionally commercial activities from those directly linked to the party-state's agendas for social control, indigenous innovation and military modernisation.

China seeks to take full advantage of the dual-use nature of AI technologies through a national strategy of 'military–civil fusion' (军民融合). This high-level agenda is directed by the CCP's Military–Civil Fusion Development Commission (中央军民融合发展委员会) under the leadership of President Xi Jinping himself.[78] Through a range of policy initiatives, China intends to ensure that advances in AI can be readily turned to dual-use applications to enhance national defence innovation. Although the effective implementation of military–civil fusion in AI may involve major challenges, this approach is presently advancing the creation of mechanisms and institutions that can integrate and coordinate R&D among scientific research institutes, universities, commercial enterprises, the defence industry and military units.[79] For instance, in June 2017, Tsinghua University announced its plans to establish a Military–Civil Fusion National Defence Peak Technologies Laboratory (清华大学军民融合国防尖端技术实验室) that will create a platform for the pursuit of dual-use applications of emerging technologies, especially AI.[80] Notably, in March 2018, China's first 'national defence science and technology innovation rapid response small group' (国防科技创新快速响应小组) was launched by the CMC Science and Technology Commission in Shenzhen,[81] and is intended to 'use advanced commercial technologies to serve the military.'[82]

China's AI 'national champions' may often be engaged in support of this agenda of military-civil fusion. Notably, in January 2018, Baidu and the 28th Research Institute of the China Electronics Technology Group's (CETC), a state-owned defence conglomerate, established the Joint Laboratory for Intelligent Command and Control Technologies (智能指挥控制技术联合实验室), located in Nanjing.[83] The CETC 28th Research Institute is known as a leading enterprise in the development of military information systems, specializing in the development of command automation systems,[84] and it seeks to advance the use of new-generation information technology in defence 'informatization' (信息化).[85] This partnership is directly linked to China's national strategy of military-civil fusion, leveraging the respective advantages of CETC and Baidu to take advantage of the potential of big data, artificial

intelligence, and cloud computing. Going forward, the new joint laboratory will focus on increasing the level of 'intelligentization' (智能化) in command information systems, as well as designing and developing new-generation command information systems 'with intelligentization as the core.' Baidu's involvement in this new laboratory reflects its active contribution to military-civil fusion, a strategy that is resulting in a further blurring of boundaries between commercial and defence developments.

Policy considerations and recommendations

There is no single or simple solution, and policy responses must take into account the inherent complexities of these global dynamics, which necessitate highly targeted and nuanced measures to mitigate risk.[86] At the same time, real and serious concerns about China's exploitation of the openness of our democracies must not lead to reactive or indiscriminate approaches that could cause collateral damage to the inclusivity and engagement that are critical to innovation. The benefits of scientific collaboration are compelling, and continued cooperation should be supported, with appropriate awareness and safeguards. In future, the quest to achieve an advantage in emerging technologies will only intensify, and the US and Australia must also look to enhance their own competitiveness in these strategic technologies.[87] The options for policy response include, but aren't limited to, the measures detailed below.

Policy recommendation: Strengthen targeted, coordinated countermeasures.

1. Review recent and existing research and commercial partnerships on strategic technologies that involve support and funding from foreign militaries, governments or state-owned/supported enterprises, evaluating the dual-use risks and potential externality outcomes in each case.
   - Evaluate early-stage research to determine the likelihood that it may turn out to have disruptive dual-use implications in the future.
   - Present a public report with findings and recommendations to raise awareness and ensure transparency.
   - Continue to push back against forced tech transfer in joint ventures.[88]
2. Explore updates and revisions to national export controls, defence trade controls and investment review mechanisms that take into account the unique challenges of dual-use commercial technologies; communicate those updates clearly and publicly to relevant stakeholders.
   - Share lessons learned and pursue coordination with allies and partners to account for the global scope and scale of these dynamics.
   - Ensure that these restrictions are applied to sensitive datasets associated with AI development, including data used for training purposes.

3. Engage in visa screening of foreign nationals who plan to study or research sensitive or strategic technologies, targeting scrutiny on the basis of whether or not students or researchers have direct and clear connections to foreign militaries, governments or intelligence services.

- Deny visas to those who are determined to be likely to leverage their studies or research in support of a foreign military that is not a security partner.
- Incorporate an independent review mechanism into the process to assess evidentiary standards and mitigate risks of bias in visa determinations.

4. Identify organisations engaging in talent recruitment that are linked to the Chinese central and local governments or to the CCP, and require their registration as foreign agents where appropriate.

5. Enhance counterintelligence capabilities, particularly by augmenting language and technical expertise.

Policy recommendation: Encourage best practices and safeguards for risk mitigation in partnerships and collaborations, with a particular focus on universities.

6. Introduce stricter accountability and reporting requirements, managed by departments of education, which make transparent international sources of funding for research strategic technologies

7. Engage in outreach to companies, universities and think tanks in order to highlight the potential for risk or unintended externalities in joint ventures and partnerships, including through developing and presenting a series of case studies based on past incidents.

8. Propose best practices for future academic collaborations and commercial partnerships, including transparency about the terms for scientific data and intellectual property, as well as clear standards on ethics and academic freedom.

- Identify favourable domains to sustain open collaboration and engagement, such as issues of safety and standards.

9. Introduce, or where appropriate adjust, policies or guidelines restricting those who work for national or military research institutes and laboratories or receive public funding at a certain level from organisations accepting funding from or collaborating with a foreign military, state-owned enterprise or ‘national champion’ that is not an ally.

Policy recommendation: Go on the offensive through policies to enhance national competitiveness in technological innovation.

10. Increase and commit to sustaining funding for basic research and the long-term development of AI technologies.

11. Prioritise improving the accessibility and affordability of STEM education at all levels, including creating new scholarships to support those studying computer science, AI and other priority disciplines.

12. Sustain openness to immigration, welcoming graduating students and talented researchers, while potentially offering a fast-track option to citizenship.

13. Pursue closer public–private partnerships through creating new incubators and institutions that create a more diverse and dynamic community for innovation.[89]

- Encourage dialogue and engagement between the tech and defence communities on issues of law, ethics and safety.

14. Explore the expansion of alliance coordination and cooperation in defence innovation, including collaboration in research, development and experimentation with new technologies and their applications.

15. Engage with like-minded nations to advance discussions of AI ethics and standards, as well as potential normative and governance frameworks.

Notes

1 Elsa B Kania, 'The pursuit of AI is more than an arms race', *Defense One*, 19 April 2018, online.

2 Kai-Fu Lee, *AI superpowers: China, Silicon Valley, and the new world order*, Houghton Mifflin Harcourt, 2018, forthcoming.

3 For prior writing on these issues, see Elsa Kania, 'Tech entanglement—China, the United States, and artificial intelligence', *Bulletin of the Atomic Scientists*, 5 February 2018, online.

4 For a detailed study on these issues, see Office of the United States Trade Representative, Executive Office of the President, *Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974*, 22 March 2018, online.

5 Throughout this policy paper, I use the concept of 'entanglement' to characterise the close linkages and range of mechanisms for engagement in the research, development and commercialisation of technologies, particularly in the context of AI. In historical perspective, entanglement, whether in alliances or economics, has proven to be both a factor restraining conflict and a major source of friction.

6 'US tech companies and their Chinese partners with military ties', *New York Times*, 30 October 2015, online.

7 Clive Hamilton, Alex Joske, 'Australian universities are helping China's military surpass the United States', *Sydney Morning Herald*, 27 October 2017, online.

8 Josh Chin, Clément Bürge, 'Twelve days in Xinjiang: how China's surveillance state overwhelms daily life', *Wall Street Journal*, 19 December 2017, online.

9 For the purposes of this paper, I target the proposed policy responses to the context of the US and Australia, but the suggested responses are intended to be applicable to other liberal democratic states.

10 These screenings should not extend to outright restrictions or unwarranted discrimination on the basis of nationality. For a compelling perspective on the imperative of keeping the door open to foreign scientists, read Yangyang Cheng, 'Don't close the door on Chinese scientists like me', *Foreign Policy*, 4 June 2018, online.

11 For a notable report on these concerns, see Michael Brown, Pavneet Singh, *China's technology transfer strategy: how Chinese investments in emerging technology enable a strategic competitor to access the crown jewels of US innovation*, Defense Innovation Unit Experimental (DIUx), January 2018, online.

12 'CFIUS reform: House and Senate committees unanimously clear bills that would greatly expand CFIUS authority', *Lexology*, 1 June 2018, online. National/State Security Law of the People's Republic of China [中华人民共和国国家安全法], 7 July 2015, online. For further discussion of the concept of 'state security', see Samantha Hoffman, 'China's state security strategy: "everyone is responsible"', *The Strategist*, 11 December 2017, online.

13 For an interview that describes the campaign from the perspective of an organiser, see 'Tech workers versus the Pentagon', *Jacobin*, 6 June 2018, online.

14 For a discussion of these plans and policies, see Elsa Kania, 'China's AI talent arms race', *The Strategist*, 23 April 2018, online.

15 Kania, 'China's AI talent arms race'.

16 Fan Yang, 'Surveying China's science and technology human talents programs', *Study of Innovation and Technology in China*, 2015, online.

17 For insights on the linkages between Silicon Valley and China, see Matt Sheehan's commentaries on the subject, including 'Silicon Valley's China paradox', *Macro Polo*, 26 June 2017, online.

18 See 'Baidu, USA', *LinkedIn*, online; 'China's Baidu increases US presence with new Silicon Valley office', *South China Morning Post*, 25 March 2017, online.

19 Bien Perez, '"China Brain" project seeks military funding as Baidu makes artificial intelligence plans', *South China Morning Post*, 3 March 2015, online; 'Li Yanhong: Establishing the "China Brain" plan to promote our nation's AI development' [李彦宏：设立"中国大脑"计划推进我国人工智能发展], *Xinhua*, 9 March 2015, online.

20 'China's Baidu buys US computer vision startup amid AI push', *Reuters*, 13 April 2017, online; Ingrid Lunden, 'Baidu acquires natural language startup Kitt.ai, maker of chatbot engine ChatFlow', *Tech Crunch*, 5 July 2017, online.

21 Lunden, 'Baidu acquires natural language startup Kitt.ai, maker of chatbot engine ChatFlow'.

22 'China's Baidu increases US presence with new Silicon Valley office', *South China Morning Post*, 25 March 2017, online.

23 The official website of the project, online. For more reporting on the launch of this program, see 'Baidu pledges to design your driverless car to "know you, and be your companion"', *South China Morning Post*, 15 August 2017, online.

24 "China Electronics Science and Technology Group and Baidu Company established the "Joint Laboratory for Intelligent Command and Control Technology" to promote military-civil fusion in the field of new technologies" [中国电科28所与百度公司成立"智能指挥控制技术联合实验室"推动军民融合向新技术领域纵深迈进], January 23, 2018, online.

25 Justina Crabtree, 'Google's next AI research center will be its first on the African continent', *CNBC*, 14 June 2018, online.

26 Jeff Dean, Moustapha Cisse, 'Google AI in Ghana', *The Keyword*, online.

27 Fei-Fei Li, 'Opening the Google AI China Center', *The Keyword*, 13 December 2017, online.

28 Fei-Fei Li, 'Opening the Google AI China Center'.

29 For further details on these incidents, see Erica Naone, 'Google reveals Chinese espionage efforts', *MIT Technology Review*, 13 January 2010, online.

30 For context, including the rationale from top current and former leaders at Google, see 'Google has a new plan for China (and it's not about search)', *Bloomberg*, 30 October 2017, online.

31 Sundar Pichai, 'AI at Google: our principles', *The Keyword*, 7 June 2017, online.

32 For one argument about the moral dimension of this issue, see Matt Sheehan, 'Google China 2.0 and the ethics of AI engagement', *Macro Polo*, 17 January 2018, online.

33 *State Council notice on the issuance of the New Generation AI Development Plan* [国务院关于印发新一代人工智能发展规划的通知], 20 July 2017, online.

34 *MIIT notice regarding the release of the Three Year Action Plan to Promote the Development of New-Generation Artificial Intelligence Industry (2018–2020)* [工业和信息化部关于印发《促进新一代人工智能产业发展三年行动计划 (2018–2020年) 》的通], 14 December 2017, online.

35 Elsa Kania, 'China's AI agenda advances, *The Diplomat*, 14 February 2018, online.

36 *State Council notice on the issuance of the New Generation AI Development Plan.*

37 'Scientific and technological innovation, a powerful engine for a world-class military' [科技创新 · 迈向世界一流军队的强大引擎], *Xinhua*, 15 September 2017, online.

38 William C Hannas, James Mulvenon, Anna B Puglisi, *Chinese industrial espionage: technology acquisition and military modernisation*, Routledge, 2013.

39 'Xi Jinping: Comprehensively advance an innovation driven development strategy, promote new leaps in national defence and military construction' [习近平 : 全面实施创新驱动发展战略 推动国防和军队建设实现新跨越], *Xinhua*, 13 March 2016, online. See also the official strategy released on innovation-driven development: 'CCP State Council releases the "National Innovation-Driven Development Strategy Guidelines"' [中共中央 国务院印发《国家创新驱动发展战略纲要》], *Xinhua*, 19 May 2016, online.

40 *State Council's several opinions regarding comprehensively strengthening basic research* [国务院关于全面加强基础科学研究的若干意见], 31 January 2018, online.

41 For more context on talent plans, see Liming Salvino, 'China's talent recruitment programs: the road to a Nobel Prize and world hegemony in science?', *Study of Innovation and Technology in China*, 2015, online.

42 For an example in Silicon Valley, see, for instance, 'Torch Hi-tech Zone Overseas Offshore Innovation Base (Silicon Valley) signing and opening ceremony held' [火炬高新区海外离岸创新基地 (硅谷) 签约暨揭牌仪式举行], *Xiamen Daily*, 30 September 2017, online.

43 *State Council notice on the issuance of the New Generation AI Development Plan.*

44 Paul Triolo, Jimmy Goodrich, 'From riding a wave to full steam ahead', *New America*, 28 February 2018, online.

45 Jimmy Goodrich, 'China's 13th Five-Year Plan: opportunities and challenges for the US semiconductor industry', written testimony prepared for the US–China Economic and Security Review Commission hearing on China's 13th Five-Year Plan, 27 April 2016, online.

46 See, for instance, Keshia Hannam, 'Four US engineers charged with trying to steal chip designs for a Chinese startup', *Fortune*, 7 December 2017, online.

47 *State Council notice on the issuance of the New Generation AI Development Plan.*

48 *Ibid.*

49 The subsidiary in question is as the CETC Software Information Services Co., Ltd. (中电科软件信息服务有限公司). See "About Us," online.

50 Some of the other notable collaborations and partnerships in Australia include the following. During 2011 and 2012, the University of Technology Sydney established five research centres with Chinese universities, including the UTS – Shanghai Jiaotong University Joint Research Centre for Intelligent Systems, the UTS – Beijing Institute of Technology Joint Research Centre for Data Mining and Service Technology, and the UTS – Tsinghua University Joint Research Centre for Quantum Computation and Artificial Intelligence. As of 2017, the UTS – Northwestern Polytechnical University International Joint Laboratory for Digital Media and Intelligent Networks, which will work on research directions including AI, computer vision, machine learning, pattern recognition, image processing, was also established. Each of these Chinese partner universities is known to engage in some military and defence-related R&D. In April 2016, the Torch Innovation Precinct at the University of New South Wales was established as a joint China–Australia science and technology partnership, receiving $100 million in funding, including for research on military-relevant technologies, including unmanned systems. As of June 2017, the University of Sydney launched a new $7.5 million research centre, led by Professor Dacheng Tao, who has worked extensively with PLA researchers, in partnership with world-leading robotics company UBTECH Robotics, to explore AI research.

51 Danielle Cave, Brendan Thomas-Noone, 'CSIRO cooperation with Chinese defence contractor should raise questions', *The Guradian*, 3 June 2017, online.

52 *CETC: a complex data condition based public security online video retrieval system*, University of Technology Sydney, online.

53 Clive Hamilton, Alex Joske, 'Australian universities are helping China's military surpass the United States', *Sydney Morning Herald*, 27 October 2017, online. I am indebted to Alex Joske for his insights and excellent research on these issues.

54 'Huawei in America: university partners', Huwei, online.

55 'By 2030, the "One Belt, One Road" science and technology cooperation network system will be basically established' [2030年将基本建成 "一带一路" 科技合作网络体系], *Economics Daily*, 10 May 2017, online; 'Qingdao's Science and Technology "bringing in" and "going out"' [青岛科技的 "引进来" 和 "走出去"], *Jiaodong*, 19 May 2018, online.

56 'Vice Minister Li Meng led a delegation to visit Greece, Sweden and Denmark' [李萌副部长率团访问希腊、瑞典、丹麦], Ministry of Science and Technology, 12 June 2018, online.

57 For a potential example of these dynamics, see Chinese funding for the Torch Innovation Precinct at the University of New South Wales. Thanks so much to Alex Joske for raising this point.

58 'Qingdao's Science and Technology "bringing in" and "going out"'.

59 For a discussion of the legal questions that this process raises, see 'China publishes final rules on the National Security Review of Foreign Investment in Chinese Companies', *Jones Day*, September 2011, online; 'National security review creates FDI hurdle', *Covington and Burling LLC*, 13 July 2015, online; National/State Security Law of the People's Republic of China. For further discussion of the concept of 'state security', see Hoffman, 'China's state security strategy: "everyone is responsible"'.

60 'State Council General Office regarding measures for the administration of scientific data' [国务院办公厅关于印发科学数据管理办法的通知], 2 April 2018, online.

61 For discussion and reactions to the policy, see Dennis Normile, 'China asserts firm grip on research data', *Science*, 9 April 2018, online.

62 'China recruits Baidu, Alibaba and Tencent to AI "national team"', *South China Morning Post*, 21 November 2017, online.

63 'National Development and Reform Commission: Baidu to lead, BAT to build indigenous AI laboratories [发改委：百度牵头，BAT筹建"国字号"人工智能实验室], *EET*, 22 February 2017, online; 'National Engineering Laboratory of Deep Learning Technologies and Applications unveiled at Baidu' [深度学习技术及应用国家工程实验室在百度揭牌], *Xinhua*, 2 March 2017, online.

64 'Cognitive intelligence has a state key laboratory' [认知智能有了国家重点实验室], *Xinhua*, 21 December 2017, online.

65 'AI "national team" Xiong'An debut! Will change your life' [人工智能"国家队"雄安登场！将改变你的生活], *Xiong'an*, 30 November 2017, online.

66 'AI "national team" Xiong'An debut! Will change your life'.

67 Charlotte Gao, 'The CCP vows to "lead everything' once again", *The Diplomat*, 28 October 2017, online; '19th Party Congress "Resolution on the Constitution of the People's Republic of China (Amendment)"' [十九大关于《中国共产党章程（修正案）》的决议], *Xinhua*, 24 October 2017, online.

68 Emily Feng, 'Chinese tech groups display closer ties with Communist party', *Financial Times*, 10 October 2017, online.

69 David Bandurski, 'Tech firms tilt toward the party', *China Media Project*, 2 May 2018, online.

70 'Internet companies "red flags": they are the party secretaries of BAT' [互联网公司"红旗谱"：他们是BAT公司的党委书记], 20 March 2017, online.

71 '35 websites in Beijing conducted their first report on party building work for the first time' [北京市35家网站首次进行基层党建工作述职], 19 March 2017, online.

72 See his biography and background as presented in English online.

73 '35 websites in Beijing conducted their first report on party building work for the first time'.

74 For a great discussion of these tensions, see Danielle Cave, 'Huawei highlights China's expansion dilemma: espionage or profit?', *The Strategist*, 15 June 2018, online.

75 Michael Martina, 'In China, the party's push for influence inside foreign firms stirs fears', *Reuters*, 24 August 2017, online.

76 *State Council notice on the issuance of the New Generation AI Development Plan.*

77 Samantha Hoffman, 'Managing the state: social credit, surveillance and the CCP's plan for China', *China Brief*, 17 August 2017, online; 'China: big data fuels crackdown in minority region', *Human Rights Watch*, 26 February 2018, online.

78 'Military–Civil Integration Development Committee established' [军民融合发展委成立], *Xinhua*, 23 January 2017, online.

79 *State Council notice on the issuance of the New Generation AI Development Plan.*

80 'Tsinghua starts to establish the Military–Civil Fusion National Defense Peak Technologies Laboratory' [清华启动筹建军民融合国防尖端技术实验室], *China Education Report*, 26 June 2017, online.

81 Although the US and Australian governments can build upon and look to the precedents of arms control and export control regimes, it's also important to recognise that these existing frameworks and paradigms can be ill-suited to the challenge of technologies in which advances are driven by academic and commercial enterprises, where research is often open-sourced and readily available, and where competition for top talent extends across borders.

82 This team will leverage 'the innovation advantages of the Shenzhen Special Economic Zone to rapidly respond to the needs of national defence science and technology innovation through various forms and accumulate experience in promoting the formation of a flexible and highly efficient defence technology innovation value chain'.

83 "China Electronics Science and Technology Group and Baidu Company established the "Joint Laboratory for Intelligent Command and Control Technology" to promote military-civil fusion in the field of new technologies" [中国电科28所与百度公司成立"智能指挥控制技术联合实验室"推动军民融合向新技术领域纵深迈进], January 23, 2018, online.

84 Ibid.

85 For more context on informatization, see: Elsa Kania and John Costello, "China's Quest for Informatization Drives PLA Reforms," *The Diplomat*, 4 March 2017, online.

86 These policy responses are intended to be generalised so as to be applicable to the US, Australia and other countries confronting comparable challenges.

87 This policy paper concentrates on AI, but similar dynamics are in play in the cases of other emerging technologies, including biotechnology and quantum information science.

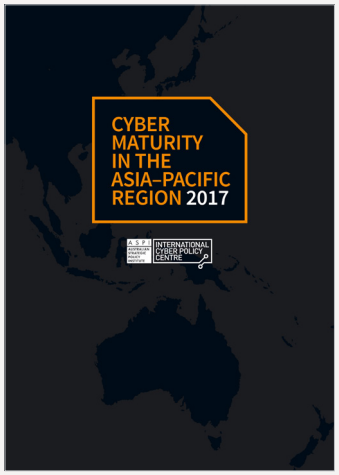
88 For more on this issue, see, for instance, Lee Branstetter, *China's 'forced' technology transfer problem—and what to do about it*, US–China Economic and Security Review Commission, 31 May 2018, online.

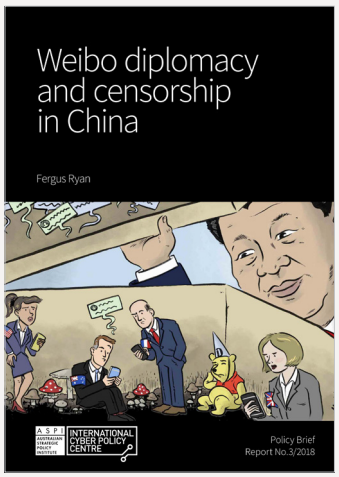
89 For example, SOFWERX is a great example of an incubator that brings together a unique and dynamic community to advance defence innovation. For further details, see Stew Magnuson, 'SOFWERX: newest acquisition tool for special operators', *National Defense*, 1 May, 2016, online.

Acronyms and abbreviations

AI	artificial intelligence
CCP	Chinese Communist Party
CFIUS	Committee on Foreign Investment in the US
PLA	People's Liberation Army
R&D	research and development
SVAIL	Silicon Valley Artificial Intelligence Laboratory
UTS	University of Technology Sydney

Some previous ICPC publications





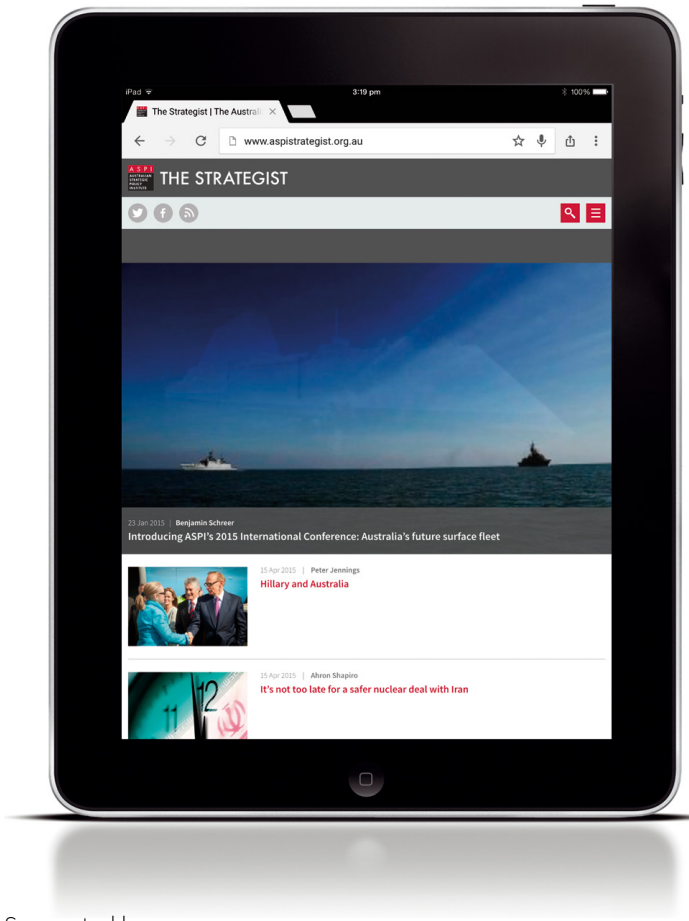
WHAT'S YOUR STRATEGY?

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.

facebook.com/ASPI.org

@ASPI_org



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Supported by

LOCKHEED MARTIN THALES KPMG

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE