TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

VOLUME 26 SPRING 2024

Artificial Intelligence and Regional Security in the Western Pacific

Michael Glanzel*

The rise of artificial intelligence (AI) has produced transformational disruptions in national security landscapes across the globe. The world's two leading powers—the United States and China—have both made heavy investments in developing and implementing AI for defense-related purposes. From creating AI-powered cyber defense tools to using AI to enhance the capabilities of existing weapons systems (such as long-range artillery), both nations have begun the process of heavily integrating AI into their militaries. The countries that sit at the fault line of this development will be those that also sit at the intersection of the growing tension between the United States and China: the states of the Western Pacific. Stretching from Japan in the North to Australia in the South, the Western Pacific covers a vast stretch of territory and harbors some of the most technologically innovative and advanced economies in the world. This Article seeks to explore the state of law and policymaking with respect to national security-related AI in the region. I argue that while some advances have been made, the region is largely failing to keep up. No nation has produced a comprehensive regulatory framework to deal with malicious foreign AI; spending on defense-related AI has lagged; limited policies have been implemented to promote AI integration and development in national militaries; and few regional defense partnerships have emerged on the issue. I posit that there is immense opportunity for the region to develop such policies and laws—and that failure to do so will place regional security in potentially dangerous waters.

* © 2024 Michael Glanzel. Judicial Law Clerk to Judge Lawrence E. Kahn, U.S. District Court for the Northern District of New York. Incoming Judicial Law Clerk to Judge Eric L. Clay, U.S. Court of Appeals for the Sixth Circuit. Former Associate at Latham & Watkins LLP in Washington, D.C. Harvard Law School, J.D. 2021; Cornell University, B.A. 2018.

I. INTRODUCTION

When OpenAI launched ChatGPT in November 2022, much of the globe's business and technology media became fixated on the rise of artificial intelligence (AI). Popular news outlets, social media, and respected figures began to proclaim the emergence of AI as "revolutionary"[1] and that a "brave new world" had emerged.[2] Yet ChatGPT is only a small part of the AI revolution—a revolution that far pre-dates November 2022. The issues that AI present have long been at the center of discussions involving the intersection of technology, business, ethics, and law. Among the most pressing of issues that has garnered a high degree of attention is the intersection of AI and national security. Many have noted that the development of AI poses important

1. Bill Gates, *The Age of AI has Begun*, GATESNOTES (Mar. 21, 2023), https://www.gatesnotes.com/The-Age-of-AI-Has-Begun [https://perma.cc/B5TU-YRCA].

2. Meaghan Johnson, *A Brave New World: ChatGPT's Potential to Reshape the Financial Services Landscape*, FORBES (Mar. 20, 2023, 10:00 AM), https://www.forbes.com/sites/meaghanjohnson/2023/03/20/a-brave-new-world-chatgpts-potential-to-reshape-the-financial-landscape/?sh=c7afd8764048.

national security threats and opportunities, with the U.S. Department of Defense claiming that AI "will transform the character of warfare."[3] Within the legal community, much of the national security conversation has been focused on the ethical dilemmas posed by AI and how AI regulation can be used as to enhance cybersecurity.[4] Yet much of the scholarship has been squarely focused on the United States. Given that the United States is widely viewed as the global leader in AI development[5] and that AI competition with China has engendered alarm,[6] it is unsurprising that American policy and lawmaking has dominated national security scholarship.

There is, however, an important conversation to be had regarding the national security implications of AI beyond the shores of the United States. And there is perhaps no more important region of the world to consider than the Western Pacific. Though the region has largely been a paragon of peace and stability for the last forty years, increasing tension between an expansionist China and its wary neighbors has produced a tense and increasingly fluid security environment. And given that the region is home to some of the world's greatest technology developers, one cannot ignore how AI will play a role in regional tensions.

This Article seeks to examine the degree to which AI law and policymaking has been employed by nations in the Western Pacific to advance national security aims and ward off Chinese aggression. Specifically, this Article looks at whether and how nations in the Western Pacific have developed AI regulatory schemes and policy positions to counter growing security concerns related to China. When discussing the Western Pacific, I focus on a wide range of states stretching from Japan and South Korea in the North, to the Philippines in the East, to Australia and New Zealand in the South, and to Vietnam in the West. While China

3. David Vergun, *Experts Predict Artificial Intelligence Will Transform Warfare*, U.S. DEP'T OF DEF. (June 5, 2020), https://www.defense.gov/News/News-Stories/article/article/2209480/experts-predict-artificial-intelligence-will-transform-warfare/ [https://perma.cc/8ENN-H9XA].

4. *See*, *e.g.*, Matthew Ivey, *The Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers*, 33 GEO. J. LEGAL ETHICS 109, 111 (2020); Theodore Bruckbauer, *CFIUS and A.I.: Defending National Security While Allowing Foreign Investment*, 4 GEO. L. TECH. REV. 279, 294 (2019).

5. *See* Paul Scharre, *To Stay Ahead of China in AI, the U.S. Needs to Work with China*, TIME (Apr. 18, 2023, 1:00 AM), https://time.com/6272400/us-china-ai-competition/ ("The U.S. currently leads in AI.").

6. *See* Vera Bergengruen, *Tech Leaders Warn the U.S. Military Is Falling Behind China on AI*, TIME (July 18, 2023, 5:19 PM). https://time.com/6295586/military-ai-warfare-alexandr-wang/.

is generally considered part of the Western Pacific, this Article focuses primarily outside of the Chinese context. Thus, when referring to the Western Pacific, I largely exclude references to China.

Throughout the Article, I often refer to two types of national-security-related AI law and policymaking: defensive and offensive. Defensive law and policymaking involves the development of legal restrictions and incentives to protect domestic security. This involves the use of legal tools to place guardrails on AI development that prevent the introduction and spread of malevolent foreign AI and promote the development of AI to protect critical infrastructure, defense systems, and democratic institutions from foreign interference or attack. Offensive law and policymaking, by contrast, is the creation of legal systems to encourage the development of weapons and systems to be used against foreign adversaries.

I argue that much of the Western Pacific has thus far failed to develop serious legal regimes to promote AI development in the national security space. Some countries—primarily, Australia, Japan, South Korea, and Taiwan—have worked to develop rough and early-stage sketches of such regimes. Others—such as New Zealand, Vietnam, and the Philippines—seem almost agnostic to the national security implications of AI. I point out that this risks the Western Pacific falling dangerously behind in the growing security contest with China, ultimately resulting in increased dependence on U.S.-based AI. Further, this Article highlights that many of these nations have the capacity to develop AI-based national security systems and that global security would benefit from a diversity of such programs.

Part II of this Article, "The AI-National Security Landscape," outlines in broad strokes how AI has become an important factor in national security. I briefly discuss how AI has become a crucial factor in national security decision making in the United States and China and how both states have begun to develop a web of legal regimes to deal with the security issues at stake. I then turn to China's role in the Western Pacific, examining how its development of AI presents major defensive threats to its neighbors in the region.

Part III, titled "The Current State of AI Law and Policymaking," looks at what steps Western Pacific states have taken to develop national-security-related AI laws and policies. This Part focuses primarily on the four states that have made large investments in national security-related AI: Australia, Japan, South Korea, and Taiwan. I then discuss the weaknesses facing the region, and explicitly highlight that many states

have failed to address defense-related AI law and policymaking in any meaningful way.

Part IV, "Opportunities for Development," outlines what measures Western Pacific nations can take and how those measures will be beneficial in the long run. I highlight that failure to create strong AI regulatory schemes risks falling behind in the AI race, ultimately leading to greater U.S. dependence. I further note that many of these countries have the capacities to establish strong legal tools and institutions to promote AI, given the highly advanced technical capabilities of the economies of the region. I also caution that certain legal troubles, such as international human rights law, may present significant challenges to AI development.

II. THE AI-NATIONAL SECURITY LANDSCAPE

The intersection between AI and national security currently feels like a fast-moving, every-changing drama with two primary actors: the United States and China. Both states have placed enormous effort into enhancing AI for national security purposes, and both have developed robust and growing legal and policy infrastructures to promote such progress. These developments will have enormous consequences for the states of the Western Pacific and have already heavily influenced the shape and scope of AI progression in the region. This Part of the Article seeks to outline the AI tension that exists between the United States and China, the legal and policy schemes that both have developed, and the growing threats facing the states of the Western Pacific.

A. An AI Arms Race?

The launch of ChatGPT produced a barrage of doomsday headlines from major publications, with one *New York Times* headline asking, "How Could A.I. Destroy Humanity?"[7] Above-the-fold commentary in the AI-related national security space has been equally apocalyptic, with many worrying that a devastating AI "arms race" is brewing between the world's greatest powers: the United States and China. In a May 2023 article, the *Bulletin of the Atomic Scientists* likened the current

7. Cade Metz, *How Could A.I. Destroy Humanity?*, N.Y. TIMES (June 10, 2023), https://www.nytimes.com/2023/06/10/technology/ai-humanity.html.

development of AI-based weaponry to the "Cold War nuclear arms race."[8]

While this commentary may be eye-grabbing, it obscures the very complicated reality of the role played by AI in the growing security tensions facing the world's two greatest powers. The development of AI represents a fundamentally new challenge to national security and defense officials given the unprecedented nature of the technology. Unlike past technological developments in the defense space, AI is not a new or improved weapon that can easily be employed on the battlefield or used to protect the homeland. Paul Scharre provides the following explanation of the uniqueness of AI: "To begin with, AI is not a weapon. AI is a general-purpose enabling technology with myriad applications. It is not like a missile or a tank. It is more like electricity, the internal combustion engine, or computer networks."[9] For this reason, many have scoffed at the notion that an "AI arms race" is developing between the United States and China. If AI is not a weapon, the argument goes, then it cannot be said that AI's development and expansion by rival powers constitutes an arms race.[10]

Even though the growth of AI in the defense space is not necessarily reflective of a traditional "arms race," it has nevertheless been an area of important development for national security officials in the United States and China. Both nations have undertaken major steps to expand their respective AI capacities in response to increased geopolitical tension and competition with each other. Many of these steps have been achieved through lawmaking—such as restrictive regulations, enhanced funding for research, and expansion of the power and scope of certain national agencies—which has in turn worked to develop both defensive and offensive capabilities.

In the defensive realm, China has undertaken some of the boldest measures to restrict the presence of malevolent AI. In July 2023, China

8. Will Henshall, *How Politics and Business Are Driving the AI Arms Race with China*, BULL. ATOMIC SCIENTISTS (May 12, 2023), https://thebulletin.org/2023/05/how-politics-and-business-are-driving-the-ai-arms-race-with-china/ [https://perma.cc/4ASM-J6LP].

9. Paul Scharre, *Debunking the AI Arms Race Theory*, 4 TEX. NAT'L SEC. REV. 121, 122 (2021).

10. *See, e.g.*, *id.*; Alexander Pascal & Tim Hwang, *Artificial Intelligence Isn't an Arms Race*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Dec. 11, 2019), https://carnegieendowment.org/2019/12/11/artificial-intelligence-isn-t-arms-race-pub-80610 [https://perma.cc/R64H-9TAF] ("Yet as technology, AI does not naturally lend itself to this framework [the race narrative] and is not a strategic weapon."); Heather M. Roff, *The Frame Problem: The AI "Arms Race" Isn't One*, BULL. ATOMIC SCIENTISTS (Apr. 29, 2019), https://thebulletin.org/2019/04/the-frame-problem-the-ai-arms-race-isnt-one/ [https://perma.cc/4XV7-YVYR].

released a new regulatory framework for generative AI,[11] and it is among one of the most sweeping and comprehensive AI governance schemes in the world. For example, Article 17 of the law requires those companies that provide generative AI services "with public opinion properties or the capacity for social mobilization" to apply to the Cyberspace Administration of China for "security assessments."[12] According to one observer, these new measures "embod[y] China's growing national security strategy, which prioritizes technological self-reliance and data security and closes off certain opportunities for foreign investment."[13] China has also undertaken strong measures to establish national agencies focused on defense-related AI. Many within China's top civilian and military posts worry that the nation has a "vulnerable dependence on imports of international technology" that gravely threatens security.[14] The development of new agencies aimed squarely at tackling this perceived vulnerability has become a focal point for national security officials. The Ministry of National Defense, for example, created two new departments in 2018 to focus on AI development: the Unmanned Systems Research Center and the Artificial Intelligence Research Center.[15] Ultimately, China's goal (as stated in its 2017 "New Generation Artificial Intelligence Development Plan") is to become both fully self-dependent and the global leader in AI technology by 2030.[16]

---

11. The U.S. Government Accountability Office provides the following definition of generative AI:

> Generative artificial intelligence (AI) is a technology that can create content, including text, images, audio, or video, when prompted by a user. Generative AI systems create responses using algorithms that are trained often on open-source information, such as text and images from the internet. However, generative AI systems are not cognitive and lack human judgment.

U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-106782, SCIENCE & TECH SPOTLIGHT: GENERATIVE AI (June 2023), https://www.gao.gov/assets/830/826491.pdf [https://perma.cc/HP3P-5H38].

12. *Interim Measures for the Management of Generative Artificial Intelligence Services*, CYBERSPACE ADMIN. OF CHINA (July 13, 2023), http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm [https://perma.cc/2TF7-JNL6].

13. Haiying Yuan, *China's AI Draft Regulation Addresses Global Concerns and Boosts National Security*, BOWER GRP. ASIA (May 25, 2023), https://bowergroupasia.com/chinas-ai-draft-regulation-addresses-global-concerns-and-boosts-national-security/ [https://perma.cc/VVY5-B8CQ].

14. Gregory C. Allen, *Understanding China's AI Strategy*, CTR. FOR NEW AM. SEC. (Feb. 6, 2019), https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy [https://perma.cc/PG3U-SJ6Z].

15. *See id.*

16. Graham Webster et al., *Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)*, STAN. UNIV.: DIGICHINA (Aug. 1, 2017), https://digichina.

The United States has also taken important defensive steps, but in some ways that differ from China's approach. Unlike China, the United States has not yet enacted sweeping regulatory reform to prevent the introduction of malicious foreign AI into the homeland.[17] And unlike China, AI regulation is not dictated from a central authority (like as China's Cyberspace Administration). Federal AI regulation is instead largely a department-specific affair, as each agency within the administrative state is generally charged with developing its own regulatory frameworks to mitigate security risks.[18] Yet the United States's defensive approach has mirrored China's in the development of a vast network of governmental organizations aimed at AI development. In 2022, for example, the Department of Defense established the Chief Digital and Artificial Intelligence Office to help advance research into key areas of national security concern.[19] The United States has also spent considerable time identifying the threats posed by AI and developing means by which the national security apparatus can respond to such concerns. One prominent example is the National Security Commission on Artificial Intelligence, which was established by Congress in 2018 to identify AI challenges and which published a comprehensive report in 2021. The report details an extensive number of national security risks posed by malevolent AI developed by foreign actors, including: manipulating voter sentiments to influence election results, stealing consumer data, disrupting cyber and communications infrastructure, and developing AI-produced biological weapons. At the same time, the report gives a litany of recommendations as to how the United States can respond, which include the development of comprehensive regulatory frameworks, strong exercise of executive power by the president, and

stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/ [https://perma.cc/N86M-KXNB].

17. *See* Ryan Heath, *China Races Ahead of U.S. on AI Regulation*, AXIOS (May 8, 2023), https://www.axios.com/2023/05/08/china-ai-regulation-race ("While American leaders fret that China might eventually overtake the U.S. in developing artificial intelligence, Beijing is already way ahead of Washington in enacting rules for the new technology.").

18. *See* Alex Engler, *The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment*, BROOKINGS (Apr. 25, 2023), https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/ [https://perma.cc/6752-RTYK].

19. *See Defense in the Digital Era: Hearing Before the Subcomm. on Cyber, Info. Tech., & Innovation of the H. Armed Servs. Comm.*, 118th Cong. 11 (2023) (statement of Dr. Craig Martell, Chief Digital & Artificial Intelligence Officer, Department of Defense), https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Martell%20Testimony.pdf [https://perma.cc/R77Z-LN8X].

aggressive investment in federal agencies and private-public partnerships.[20]

Offensively, both the United States and China have invested a high degree of governmental time, energy, and funds into research for AI-based weapons systems. In his 2018 book *Army of None: Autonomous Weapons and the Future of War*, Scharre outlines how both the United States and China have placed huge resources into developing autonomous weapons. Those weapons range the gambit from conventional arms (such as tanks) manned by AI systems to drone swarms to weaponized robots.[21]

AI-based weapons systems are perhaps the most obvious examples of AI's influence in the offensive interplay between the United States and China. But there are other mechanisms that each country is employing as well. The United States has been using the legal tools at its disposal to directly hinder China's ability to develop AI technologies. In October 2022, the Biden Administration announced a new set of controls on technology exports to China, banning the export of certain AI-related semiconductors to the East Asian giant.[22] It appears as if this was only the beginning of the Administration's attempt to hinder China's AI growth, as further export controls arrived just ten months later in August 2023.[23] China, by contrast, is suspected of engaging in widespread theft of AI technologies to bolster its own national security objectives. In July 2023, Christopher Wray, the Director of the U.S. Federal Bureau of Investigation, warned: "Nation-state adversaries, particularly China, pose a significant threat to American companies and national security by stealing our AI technology and data to advance their own AI programs and enable foreign influence campaigns."[24]

In sum, the speed and scale at which AI has transformed the national security landscape in the United States and China is profound. Both states

20. *See generally* NAT'L SEC. COMM'N ON A.I., FINAL REPORT: NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE (2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf [https://perma.cc/836N-ZV7M].

21. PAUL SCHARRE, ARMY OF NONE: AUTONOMOUS WEAPONS AND THE FUTURE OF WAR 77 (W. W. Norton & Company, 2018).

22. For a more detailed description of the regulations, *see* Gregory C. Allen, *Choking off China's Access to the Future of AI*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 11, 2022), https://www.csis.org/analysis/choking-chinas-access-future-ai [https://perma.cc/7R9N-PEWQ].

23. *See* Karen Freifeld et al., *Biden Orders Ban on Certain U.S. Tech Investments in China*, REUTERS (Aug. 10, 2023, 7:03 AM), https://www.reuters.com/world/white-house-detail-plans-restricting-some-us-investments-china-source-2023-08-09/.

24. Masood Farivar, *FBI Warns About China Theft of US AI Technology*, VOICE OF AM. (July 28, 2023, 7:24 PM), https://www.voanews.com/a/fbi-warns-about-china-theft-of-us-ai-technology/7202760.html [https://perma.cc/C7L5-B68S].

have taken aggressive steps to use their respective legal and policy regimes to either protect against malicious AI or advance offensive objectives. This is important context for the states of the Western Pacific, who live at the intersection of these two colossuses and whose own regional security will be directly impacted by these developments.

B. The AI-Based Threats Facing the Western Pacific

The Western Pacific today faces some of the greatest regional security challenges since the end of the Second World War. For nearly seventy years, the Western Pacific has enjoyed what commentators call a "long peace," defined as the period from the end of the Korean War in 1953 to the present, during which the region has largely been spared from widespread conflict.[25] Though the region was not entirely free from warfare—Vietnam's successive wars with France, the United States, and China immediately come to mind—those military engagements were largely sub-regional or bilateral in nature and did not subsume most or all of the Western Pacific.[26] This period of stability allowed the Western Pacific to generate an immense degree of societal and economic growth, with nations such as Japan and Korea becoming international leaders in technological development and nations such as Vietnam and Indonesia becoming important manufacturing hubs.[27] In recent years, however, the rise of China has threatened the long peace. China's increasing willingness to flex its military, political, and economic muscles in the region—from aggressive naval base construction in the South China Sea to increasing signals that the nation may invade Taiwan—has placed regional security in question. Further, the United States's heightened willingness to confront Chinese expansion has only worked to magnify fears in the Western Pacific.[28]

As the region has entered into a new period of increasing uncertainty, many of the region's actors have taken aggressive steps to

25. *See* Euan Graham, *Will the Western Pacific's Long Peace Endure?*, LOWY INST. (Feb. 9, 2017), https://www.lowyinstitute.org/the-interpreter/will-western-pacific-s-long-peace-endure [https://perma.cc/TS25-FLTK].

26. *See* Kevin Rudd, *Preserving Asia's Long Peace*, 10 HORIZONS, 104 (2018) ("The Vietnam war remained a sub-regional conflict, albeit devastating for the participants. Just as the 1962 Sino-Indian border war remained an exclusively bilateral affair, so did the Bangladesh Liberation War of 1971.").

27. *See id.*

28. For a more comprehensive discussion of this trend, see ASIA SOC'Y POL'Y INST., PRESERVING THE LONG PEACE IN ASIA: THE INSTITUTIONAL BUILDING BLOCKS OF LONG TERM REGIONAL SECURITY (2017), https://asiasociety.org/files/uploads/191files/LongPeaceAsia_onlinevers.pdf [https://perma.cc/H4WJ-58JY].

shore-up their respective national security apparatuses. Australia, for example, signed a trilateral security pact with the Untied States and the United Kingdom (commonly called AUKUS) in 2021, with many commentators believing that the purpose of the agreement is to deter Chinese aggression in the Western Pacific.[29] In late 2022, Japan announced a new commitment to drastically increase defense spending, putting the country on pace to have the world's third-largest defense budget by 2027.[30] Vietnam has taken efforts to establish closer relations with the United States, its one time military adversary,[31] while South Korea's President Yoon Suk-yeol campaigned heavily on closer U.S.-Korean ties during the 2022 South Korean presidential election.[32] And in August 2023, Japan and South Korea overcame many historical and cultural tensions to sign a security pact with the United States, which many observers considered to be a "historic" alliance.[33]

The explosive growth of AI has only further complicated the security picture for the Western Pacific. China's aggressive expansion of defense-related AI has caused alarm bells to ring from Tokyo to Canberra, with many fearing that Beijing will use its new tools for malicious purposes. There is perhaps no more prominent example of this than China's multifaceted employment of offensive AI against Taiwan.

C. The Threat Facing Taiwan

It is no secret that China harbors deep ambitions of making Taiwan a part of the People's Republic of China. News reports have noted that "US intelligence believes that Xi Jinping, China's leader, has ordered the

29. *See* James Curran, *Could the AUKUS Deal Strengthen Deterrence Against China—And Yet Come at a Real Cost to Australia?*, COUNCIL ON FOREIGN RELS. (Sept. 20, 2021, 2:05 PM), https://www.cfr.org/blog/could-aukus-deal-strengthen-deterrence-against-china-and-yet-come-real-cost-australia [https://perma.cc/8SB2-UM57].

30. *See* Jennifer Kavanagh, *Japan's New Defense Budget Is Still Not Enough*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Feb. 8, 2023), https://carnegieendowment.org/2023/02/08/japan-s-new-defense-budget-is-still-not-enough-pub-88981 [https://perma.cc/EJ3P-FB5K].

31. *See* Jonathan Stromseth, *A Window of Opportunity to Upgrade U.S.-Vietnam Relations*, BROOKINGS (Dec. 20, 2022), https://www.brookings.edu/articles/a-window-of-opportunity-to-upgrade-us-vietnam-relations/ [https://perma.cc/XLY8-87XH].

32. *See* Scott A. Snyder, *How South Korea's Foreign Policy Could Change Under the New President*, COUNCIL ON FOREIGN RELS. (Mar. 10, 2022, 2:42 PM), https://www.cfr.org/in-brief/south-korea-election-new-president-yoon-foreign-policy [https://perma.cc/L3N5-Y535].

33. *See Experts React: The US-Japan-South Korea Summit Was 'Historic.' But What Did it Accomplish?*, ATL. COUNCIL (Aug. 18, 2023), https://www.atlanticcouncil.org/blogs/new-atlanticist/experts-react/experts-react-the-us-japan-south-korea-summit-was-historic-but-what-did-it-accomplish/ [https://perma.cc/PTR6-BRQG].

country's military to be ready by 2027 to annex Taiwan."[34] Among China's first steps in advancing its goal to take the island is an attempt to undermine Taiwan's political institutions. One of the most deliberate examples of this can be seen in China's interference in Taiwan's 2020 presidential election, in which China employed a variety of means to sow discord among the public and weaken certain candidates. For example, reports highlighted that China engaged in widespread disinformation efforts to sow discord and confusion among the public. Chinese cyber units were suspected of covertly spreading a wide range of falsehoods on social media, such as the claim that incumbent president Tsai Ing-wen had obtained a fake doctoral degree from the London School of Economics.[35] In conducting this campaign to undermine Taiwan's 2020 elections, many believed that China made extensive use of AI. Taiwan's cybersecurity chiefs suspect that during the 2020 elections, China employed myriad AI-based schemes to enhance disinformation efforts. As one commentator noted:

> Michael Cole, editor of the Taiwan Sentinel, who has investigated Chinese influence operations, said there was "accumulating evidence that Beijing has begun experimenting with AI to generate false content and disinformation." "We're seeing the first steps towards using AI and computers to 'write' news, using a few keywords, that seems credible," he said. "We've also been seeing evidence of automation in the sharing, almost instantly, of disinformation on social media. I think AI will be the next phase in Beijing's efforts to overload and saturate the Taiwanese information environment." It is "a laboratory for China for adaptation and improvement on political warfare instruments which can then be unleashed against other targeted democratic societies," he said.[36]

34. Amy Hawkins, *Taiwan Foreign Minister Warns of Conflict with China in 2027*, THE GUARDIAN (Apr. 21, 2023), https://www.theguardian.com/world/2023/apr/21/taiwan-foreign-minister-warns-of-conflict-with-china-in-2027.

35. For a more thorough discussion of Chinese disinformation efforts during the election, see AARON HUANG, COMBATTING AND DEFEATING CHINESE PROPAGANDA AND DISINFORMATION: A CASE STUDY OF TAIWAN'S 2020 ELECTIONS 13-14 (2020).

36. Phil Sherwell, *Artificial Intelligence: China 'Uses Taiwan for Target Practice' as it Perfects Cyber-Warfare Techniques*, SUNDAY TIMES (Jan. 5, 2020, 12:01 AM), https://www.thetimes.co.uk/article/china-uses-taiwan-for-target-practice-as-it-perfects-ai-cyber-warfare-to-attack-the-west-sdn9qm8jt.

As dramatic as this development was, it was not the first time Taiwanese officials suspected Chinese AI-based influence campaigns. Some believed that such efforts started in 2019.[37]

Officials in Taiwan believe that China is poised to expand its use of AI to sow electoral confusion and disinformation. In June 2023, Taiwanese officials cautioned that "Beijing could use deepfake technology to create false allegations of electoral fraud or discredit candidates as part of its disinformation campaign to meddle in Taiwan's elections" in the future.[38] This use of AI in Taiwanese elections is an example of the nation's development of powerful offensive AI tools. It is also an important example of the threat currently facing many in the Western Pacific. AI-based weaponry contains the potential to threaten democratic institutions and processes, thus working to weaken the governments and societal cohesion. Although China's efforts to interfere in Taiwan's 2020 elections were seen as largely unsuccessful,[39] it is unclear whether this lack of success will persist into the future as Chinese weapons become more sophisticated and harder to detect.

Election interference is not the only example of China's use of AI to spread disinformation in Taiwan. Reports indicate that China has begun to use AI to launch a disinformation campaign to spread doubts about the relationship between Taiwan and the United States. As one report states: "Chinese disinformation utilizes co-opted non-Chinese media outlets and fake Web sites registered outside of Taiwan and China to pose as legitimate foreign institutions and distort real comments made by foreign officials."[40] For example, recent investigations have found that Chinese agents have used AI to generate false news stories claiming that U.S. officials have announced plans to bomb Taiwanese semiconductor facilities in the event of war between China and Taiwan.[41] Another example China's disinformation campaign is its use of AI to generate fake or altered images that sow fear among the Taiwanese public. Reports have found that Chinese social media accounts have posted altered images of

37. *See Taiwan | Chinese Cyber Threat Ahead of 2024 Elections*, DRAGONFLY INTEL. (June 13, 2023), https://www.dragonflyintelligence.com/news/taiwan-chinese-cyber-threat-ahead-of-2024-elections/ [https://perma.cc/N5G2-XSZB] ("In 2019, the authorities in Taiwan reportedly said they suspected China of using AI in influence campaigns to boost online content.").

38. Chung Li-hua & Jonathan Chin, *China Could Use AI to Meddle in Polls*, TAIPEI TIMES (June 24, 2023), https://www.taipeitimes.com/News/front/archives/2023/06/24/2003802077 [https://perma.cc/W7AJ-9K3R].

39. *See* HUANG, *supra* note 35, at 5 ("In its 2020 presidential and legislative elections, Taiwan combatted and defeated Chinese propaganda.").

40. Li-hua & Chin, *supra* note 38.

41. *Id.*

Chinese warships moving near major Taiwanese military installations and civilian populations along Taiwan's coastline.[42]

Disinformation is only one part of the multifaceted problem facing Taiwan due to China's rapidly expanding AI capacities. Another threat concerns the use of AI to enhance already existing military weapons systems—systems that could be used against Taiwan in a potential future invasion. In April 2023, news outlets concluded that China had successfully tested long-range artillery powered by AI, which dramatically increased the accuracy and precision of the weapons. The tests showed that the weapons could fire at human-sized targets nearly ten miles away and come within centimeters of the target.[43] Many note the serious risk this poses to Taiwan should China decide to take military action against the island. As one commentator states: "In a Taiwan scenario, . . . AI-powered guided artillery can take out targets in urban areas more efficiently than traditional firepower and at lower costs than missiles."[44] Reports have also indicated that AI has been used to enhance Chinese airpower. One article highlights that "variants of aircraft have been modified to be operated via remote control or potentially autonomously, perhaps to overwhelm air defenses in a potential invasion scenario against Taiwan."[45]

Taiwan has also expressed concern that AI may be used to develop powerful cyberweapons. In April 2023, National Security Bureau Director General Tsai Ming-yen cautioned that AI is already being used in "attacking or hacking into key infrastructure in Taiwan and spreading or selling stolen data online."[46] This is not surprising, given that experts based in the United States have long cautioned that China is developing AI-based weapons to conduct wide-ranging cyber operations.[47]

42. *Id.*

43. *See* Stephen Chen, *China Tests AI-Powered Long-Range Artillery that Can Hit a Person 16km Away*, S. CHINA MORNING POST (Apr. 17, 2023, 7:00 PM). https://www.scmp.com/news/china/science/article/3217334/china-tests-ai-powered-long-range-artillery-can-hit-person-16km-away.

44. Gabriel Honrada, *China Uses AI to Aim its Big Guns Against Taiwan*, ASIA TIMES (Apr. 20, 2023), https://asiatimes.com/2023/04/china-uses-ai-to-aim-its-big-guns-against-taiwan/ [https://perma.cc/7DT2-2YV8].

45. ELSA B. KANIA, BROOKINGS INST., "AI WEAPONS" IN CHINA'S MILITARY INNOVATION 4 (2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf [https://perma.cc/S7AF-BY4K].

46. Shelley Shan, *China Might Use AI to Sow Chaos: NSB*, TAIPEI TIMES (Apr. 27, 2023), https://www.taipeitimes.com/News/taiwan/archives/2023/04/27/2003798692 [https://perma.cc/KMJ6-4QSQ].

47. *See, e.g.*, AJ Vicens, *Top FBI Officials Warn of 'Unparalleled' Threat from China and AI*, CYBERSCOOP (July 26, 2023), https://cyberscoop.com/fbi-officials-cybersecurity-china-ai/

Furthermore, given that AI-based cyberattacks have already been employed by malign actors to harm critical infrastructure (such as a 2023 Russian-based attack on the U.S. Department of Energy),[48] Taiwan has good reason to fear that China might employ similar weaponry.

D. Beyond Taiwan

Taiwan is not the only nation that faces deep concerns about China's rising offensive AI capabilities. In its 2022 Annual White Paper, Japan's Ministry of Defense outlined a number of areas of development that deeply trouble Japan. The White Paper outlines that China has placed a heavy emphasis on "intelligentized warfare," which the report defines as the use of AI in warfare.[49] Among the most pressing issues in the development of this intelligentized warfare is what the report calls "cognitive warfare." This involves using AI to sow "social disorder by manipulating and disrupting the public's mentality through the deployment of 'Three Warfares' (psychological warfare, public opinion warfare, and legal warfare) and the dissemination of disinformation via social media and other means."[50] Japan's National Institute for Defense Studies created an entire report in 2022 dedicated to exploring China's use of cognitive warfare. The report details that AI can be used to fully maximize cognitive warfare, which will help to develop weapons "such as cultural propagation, public opinion induction, and biological weapons to destroy the cognitive capabilities of the opponent; protect one's cognitive capabilities; gain the initiative, control, and discourse power in cognitive space confrontations; and acquire information as well as control policy decisions that affect operations command."[51] The report

[https://perma.cc/4KAB-63EY]; Jessica Lyons Hardcastle, *US Cyber Chiefs Warn AI Will Help Crooks, China Develop Nastier Cyberattacks Faster*, THE REGISTER (Apr. 12, 2023), https://www.theregister.com/2023/04/12/us_chatgpt_threat/ [https://perma.cc/HDR2-EW8G]; Bob Violino, *Artificial Intelligence Is Playing a Bigger Role in Cybersecurity, But the Bad Guys May Benefit the Most*, CNBC (Sept. 13, 2022, 11:24 AM), https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html [https://perma.cc/7E7H-6SA8].

48. *See Cybersecurity Crisis: AI and the Attack on U.S. Energy Infrastructure*, A.I. PLAIN ENG. (June 17, 2023), https://ai.plainenglish.io/cybersecurity-crisis-ai-and-the-attack-on-u-s-energy-infrastructure-4df0859b3557.

49. JAPAN MINISTRY OF DEF., DEFENSE OF JAPAN 44 (2022), https://www.mod.go.jp/en/publ/w_paper/wp2022/DOJ2022_EN_Full_02.pdf [https://perma.cc/7Z9E-ZTZZ].

50. *Id.*

51. YAMAGUCHI SHINJI ET AL., NAT'L INST. FOR DEF. STUD., JAPAN, CHINA'S QUEST FOR CONTROL OF THE COGNITIVE DOMAIN AND GRAY ZONE SITUATIONS 46 (2022), http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf [https://perma.cc/K9AH-BRLE].

specifically highlights China's recent attempts to spread disinformation in Taiwan as a reason why Japan should be particularly concerned about China's growing cognitive warfare capabilities.[52]

In the realm of cognitive warfare, authorities have warned that China could use AI-based disinformation campaigns to drive a wedge between Western Pacific states and the United States. One set of experts noted that China's military is likely to wage a "campaign to discredit U.S. military activities or sow division with partners, including Australia and Japan."[53] Major Ian T. Brown of the U.S. Marine Corps explains how this could work. He gives the example of using AI to create fake videos regarding U.S. military personnel stationed on the Japanese island of Okinawa. According to Brown, "China could create fake videos to turn the Okinawan population and Japanese government against America" by creating depictions of U.S. Marines and sailors sexually assaulting local Okinawans.[54] This, in turn, would sow distrust between the U.S. military and the Japanese public, thus weakening one of the Western Pacific's most powerful alliances.[55] Given that the United States maintains bases across many nations in the Western Pacific (ranging from South Korea to the Philippines), it is not inconceivable that this tactic could be used in many nations throughout the region.

China might also use AI-based cognitive warfare to push misinformation that will disrupt national unity, harm elections, and sow public discord. A good example of how this is already at work can be found in the Philippines. In 2020, Facebook announced that it had discovered and banned a network of Chinese-based accounts that "coordinated inauthentic behavior on behalf of a foreign or government entity."[56] These accounts were largely fake, but had initially gone undetected because the profile pictures were generated through a sophisticated form AI designed to elude Facebook's monitors. The accounts then spread a number of posts aimed at disseminating

52. *Id.* at 10.

53. Alex Stephenson & Ryan Fedasiuk, *How AI Would—and Wouldn't—Factor Into a U.S.-Chinese War*, WAR ON THE ROCKS (May 3, 2022), https://warontherocks.com/2022/05/how-ai-would-and-wouldnt-factor-into-a-u-s-chinese-war/ [https://perma.cc/TDK5-KGJU].

54. Ian T. Brown, *Cyber's Cost: The Potential Price Tag of a Targeted "Trust Attack*,*"* 10 MARINE CORPS UNIV. J. 102, 105 (2019), https://www.usmcu.edu/Portals/218/MCUJ_10_1_Cybers%20Cost_The%20Potential%20Price%20Tag%20of%20a%20Targeted%20Trust%20Attack_Ian%20Brown.pdf [https://perma.cc/M2MW-PQZ6].

55. *Id.*

56. Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior*, META (Sept. 22, 2020), https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-china-philippines/ [https://perma.cc/8F9Q-XG2F].

propaganda and misinformation, which included "global news and current events including China's interests in the South China Sea; Hong Kong; content supportive of President Rodrigo Duterte and Sarah Duterte's potential run in the 2022 Presidential election; criticism of Rappler, an independent news organization in the Philippines; [and] issues relevant to the overseas Filipino workers."[57]

Outside of cognitive warfare, many have expressed deep concerns about China's use of AI to enhance cyberattacks. In a 2023 article in the *International Journal of Novel Research*, researchers highlighted that China's growing AI capacities would likely be used to enhance offensive cyber operations.[58] The article notes that Chinese actors have already engaged in cyberattacks, explaning that Japan and South Korea in particular have suffered from such offensives. One example is a cyberattack launched by a Chinese state-sponsored organization codenamed "Cicada," which involved "the theft of sensitive information from Japanese defense contractors, the disruption of the operations of Japanese critical infrastructure, and the compromise of Japanese government agencies and diplomatic missions."[59] Another Chinese cyberattack involved the South Korean conglomerate Lotte Corporation, in which the company was exposed to damaging malware.[60] These attacks, the article highlights, are likely increase in terms of scale, frequency, and effectiveness as AI is used to enhance these cyberweapons.[61]

In summary, the Western Pacific faces a growing security dilemma with regards to AI. The region is currently caught between—both literally and figuratively—two rival superpowers who both have invested enormous resources into developing their respective AI capabilities. At the same time, China's rise in the region has presented direct AI-based security threats. China has already used or is expected to use AI to spread

57. Taylor Hatmaker, *Chinese Propaganda Network on Facebook Used AI-Generated Faces*, TECHCRUNCH (Sept. 22, 2020, 1:27 PM), https://techcrunch.com/2020/09/22/facebook-gans-takes-down-networks-of-fake-accounts-originating-in-china-and-the-philippines/ [https://perma.cc/HR3T-7J8S].

58. Akshita Pant & Nagalaxmi M. Raman, *China's Cyber Threats Against East Asia*, 8 INT'L J. NOVEL RSCH. & DEV. 659, 662 (Apr. 2023), https://www.researchgate.net/publication/370837629_CHINA'S_CYBER_THREATS_AGAINST_EAST_ASIA [https://perma.cc/T6PG-XWD6].

59. *Id.* at 663.

60. *Id.*; *see also* John W. Little, *Combating Chinese Cyber Threats in South Korea*, BLOGS OF WAR (Feb. 23, 2023), https://blogsofwar.com/chinese-cyber-threats-against-south-korea-defense-and-collaboration-strategies/ [https://perma.cc/RKP2-AWK7].

61. Pant & Raman, *supra* note 58, at 660-61.

disinformation, develop cyberattacks, undermine alliances, and enhance already-existing weapon systems. It is because of these developments that the role of AI in national security has become an important talking point in national security circles across the Western Pacific. However, as we will see, the region currently risks falling deeply behind in the AI race.

III. THE CURRENT STATE OF AI LAW AND POLICYMAKING

As outlined above, both the United States and China have taken significant steps to establish legal and policy regimes in the national security realm that place guardrails on AI, promote AI's development, hinder adversarial AI development, or establish new agencies to oversee AI's growth. From China's 2023 announcement that established the most comprehensive generative AI regulatory scheme in the world, to both nations' investment in AI-based weapons systems, the world's two leading military and economic powers have taken enormous steps to use law and policymaking to advance defense-related AI goals. At times it can appear as if these two nations dominate the global AI scene, while the rest of the world is left as a set of supporting characters. There have been, however, important steps taken in the Western Pacific to establish laws and policies aimed at national security-related AI. Many of the region's major economic and military players—namely Australia, Japan, South Korea, and Taiwan—have taken major first steps in this arena. Yet there has been much missed opportunity in the national security space, as many nations seem to be unfocused on AI's development in defense. This Subpart of the Article seeks to highlight those areas of progress and where the region has been lacking. I note that while important advances have developed, the serious lack of investment in several crucial areas threatens to place the region behind in the AI race.

A. Current Advancements

A number of states in the Western Pacific have taken important strides in developing legal and policy frameworks to advance national security goals within the AI space. Two nations that have both undertaken great advances in this realm and have moved roughly in parallel are Japan and Australia. These two have similar security situations as both face hostility from China, maintain close ties with the United States, and are members of important defense dialogues and alliances. It is thus unsurprising that AI development has moved in tandem. Another pair of nations that has also moved to develop comparable AI law and policymaking due to similar geostrategic concerns is South Korea and

Taiwan. What separates these two nations from the rest of the region is that they both face immediate security concerns: Taiwan fears an imminent invasion from China, and South Korea maintains dangerously unstable relations with North Korea. I first sketch the developments undertaken by Japan and Australia, then outline the measures adopted by South Korea and Taiwan. I conclude by briefly touching on the advances of other states in the region.

1. Japan and Australia

Japan and Australia have emerged as two important leaders in the race to develop AI laws and policies in the national security realm. In developing AI capabilities, regulatory systems, and governmental initiatives, both nations have acted in parallel ways, as advances in one nation are in many ways mirrored by the other. This is unsurprising given that both maintain similar security situations. While neither (unlike Taiwan) maintains fears of an imminent Chinese invasion, both are wary of how China's rise threatens regional security.[62] Furthermore, both are members of key alliances with the United States: Japan and Australia are parties to the Quadrilateral Security Dialogue (the Quad); Australia is a member of the trilateral AUKUS security pact; Japan is a member of the trilateral security pact with the United States and South Korea; and both are designated as major non-NATO allies by the United States.

One of the first steps that the governments of each nation have taken is to develop new governmental agencies aimed specifically at developing AI for national security purposes. In its 2022 National Security Strategy, Japan announced that it would tackle the problems of cognitive warfare in the AI realm by creating "a new structure . . . within the government to aggregate and analyze information on disinformation and others originated abroad."[63] What exactly this "new structure" will look like and how it will operate within the government are not clear from the report, and the government does not appear to have provided more details on the plan to develop this agency. At the same time, Japan has begun looking into developing a research agency within the Ministry of Defense to produce new AI technologies. Specifically, Japan is looking to create a

62. *See* Kyoko Hatakeyama, *The Deepening Japan-Australia Security Relationship: Deterrence Against China or Alternatives to the Region?*, ASIA SOC'Y (Feb. 19, 2023), https://asiasociety.org/australia/deepening-japan-australia-security-relationship-deterrence-against-china-or-alternatives-region [https://perma.cc/4FU2-VBCN].

63. CABINET SECRETARIAT OF JAPAN, NATIONAL SECURITY STRATEGY OF JAPAN 27 (Dec. 2022), https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf [https://perma.cc/9L9G-TTWP].

"new research body modeled on a U.S. agency to support civilian technology with military applications."[64] The U.S. agency that Japan looks to model is the Defense Advanced Research Projects Agency (DARPA), which has long been a center for technological innovation within the U.S. Department of Defense. Japan is also looking to the United States's Defense Innovation Unit for inspiration, which was created in 2015 by the Pentagon "to collaborate closely with tech companies."[65] By modeling itself on these U.S. agencies, Japan hopes its new defense research arm will launch "cutting-edge projects in artificial intelligence, quantum computing and drones."[66]

Australia has taken a similar approach in creating governmental agencies—but appears to be more advanced than Japan in this area. Whereas Japan has either announced plans to develop or is actively exploring developing national security related agencies, Australia has already established such institutions. The Australian military's Joint Capabilities Group has taken a lead in establishing AI-based agencies, one of which is the recently established Defence Artificial Intelligence Centre. The goal of this agency is to "accelerate [Australia's] capability foundations and the understanding and implementation of coordinated artificial intelligence technologies across the enterprise."[67] To achieve this goal, the agency "is engaged with academia and industry in the development of future AI capabilities,"[68] and has recently signed research contracts with the University of South Australia and Deakin University.[69] Yet this is not the only agency established by the Joint Capabilities Group as the group has also established the Defence Technology Acceleration Collaboration Laboratory. The goal of this laboratory is to "better connect Defence with industry and university AI expertise" to develop and test

64. Ryo Nemoto, *Japan Eyes U.S.-Style Defense Research Agency as Tech Race Heats Up*, NIKKEI ASIA (Oct. 20, 2022), https://asia.nikkei.com/Politics/Japan-eyes-U.S.-style-defense-research-agency-as-tech-race-heats-up.

65. *Id.*

66. *Id.*

67. AUSTL. GOV'T: DEPT. OF DEF., DEFENCE DATA STRATEGY 2021-2023 35 (2021).

68. PARLIAMENT OF AUSTL., DEFENCE ANNUAL REPORT 2019-2020: SPACE-BASED INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (2021), https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Foreign_Affairs_Defence_and_Trade/DefenceAReport19-20/Report/section?id=committees%2freportjnt%2f024803%2f77861 [https://perma.cc/GW4D-J2HC].

69. *See* Media Release, Austl. Gov't: Dept. of Def., Defence Artificial intelligence research network contracts signed (Mar. 6, 2023), https://www.defence.gov.au/news-events/releases/2023-03-06/defence-artificial-intelligence-research-network-contracts-signed [https://perma.cc/87X6-XERK].

prototypes of AI-based defense capabilities.[70] The laboratory's recent studies have investigated data in intelligence gathering, virtual reality, and graphics application.[71]

Outside of the Joint Capabilities Group, various civilian offices in the Department of Defence have been established to enhance AI development. One is the Trusted Autonomous Systems Defence Cooperative Research Centre. The center is specifically aimed at leveraging expertise across other governmental agencies, academia, and private industry to produce AI-based robotics.[72] Recent research projects have included developing autonomous naval vessels, partnering with Boeing Australia to create machine learning techniques to power surveillance reconnaissance missions, and researching autonomous mine clearance technologies.[73] Another agency is the Defence AI Research Network, which works with researches across the country to develop "the broader Defence and AI ecosystems."[74]

The development of these agencies by both Australia and Japan points to another policy emphasis for each respective government: financial investment in national security-related AI research. Throughout various rounds of budget negotiations with each nation's parliaments, increasing sums of money have been allocated to AI development. Japan's financial investment in AI comes at a crucial time for the nation's defense-related budgetary policy and lawmaking. Historically, Japan has retained a relatively modest defense budget since its defeat in the Second World War and adoption of a pacifist constitution.[75] Yet in December 2022, Prime Minister Fumio Kishida's government announced a transformation in the nation's budgetary policies, committing the country to a nearly sixty percent increase in defense spending by 2027, with a

70. PETER LAYTON, DEF. A.I. OBSERVATORY, EVOLUTION NOT REVOLUTION: AUSTRALIA'S DEFENCE AI PATHWAY 16 (2022), https://defenseai.eu/wp-content/uploads/2023/01/DAIO_Study2202.pdf [https://perma.cc/7WEW-8K8K].

71. *Id.*

72. *See* AUSTL. GOV'T: DEPT. OF DEF., DEFENCE COOPERATIVE RESEARCH CENTRE PROGRAM, https://www.dst.defence.gov.au/sites/default/files/publications/documents/NGTF%20CRC%20A4%20Brochure%20LR.pdf [https://perma.cc/BR9M-FKCQ].

73. *See What We Do*, TRUSTED AUTONOMOUS SYS., https://tasdcrc.com.au/what-we-do/#mcm [https://perma.cc/V794-9EUV].

74. *About DAIRNet*, DAIRNET, https://www.dairnet.com.au/about/about-us/ [https://perma.cc/HV5A-4NRK].

75. *See*, *e.g.*, Adam P. Liff, *Policy by Other Means: Collective Self-Defense and the Politics of Japan's Postwar Constitutional Reinterpretations*, 24 ASIA POL'Y, 139 (2017); John Wright, *Japan's Self-Imposed One Percent: Does It Really Matter?*, AIR UNIV. J. INDO-PAC. AFF. (July 2022), https://media.defense.gov/2022/Jul/11/2003033518/-1/-1/1/JIPA%20-%20WRIGHT%20-%20JUL%2022.PDF [https://perma.cc/JM36-6G42].

twenty percent increase in spending from 2022 to 2023 alone.[76] A look into the 2023 budget reveals new investments in AI-based research, including allocations for the development of unmanned weapons systems and AI-based accelerated decision making.[77] Given that Japan has pledged to continue to expand its defense spending through 2027, it seems likely that defense spending on AI will increase in the coming years. Australia has also made similar investments in AI research. Over the last several years, the government has made several investments in AI, including $32 million worth of contracts in 2021 to develop defense-related AI.[78]

Both Japan and Australia have also begun to adopt policies that are aimed at at introducing AI-based weapons systems into their respective militaries. One of Japan's first forays into AI weaponry occurred in 2019 under the leadership of then-Prime Minister Shinzo Abe. The government announced a major shift in defense spending policy, declaring that Japan would begin its first major procurements of AI weapons. The purchase of these weapons was primarily aimed at developing the nation's robotic capabilities as the government specifically announced acquisitions of unmanned ariel vehicles and underwater drones.[79] According to one source, Japan's decision to implement these weapons was due "in part to compensate for [Japan's] low birthrate and population decline."[80] Since 2019, the government has continued to invest in AI-manned autonomous vehicles. In 2022, for example, the government announced plans to develop an armed drone that would "receive terrain and weather

76. *See* Jeffrey W. Hornung & Christopher B. Johnstone, *Japan's Strategic Shift is Significant, But Implementation Hurdles Await*, WAR ON THE ROCKS (Jan. 27, 2023), https://warontherocks.com/2023/01/japans-strategic-shift-is-significant-but-implementation-hurdles-await/ [https://perma.cc/JE6D-3G4Y].

77. JAPAN MINISTRY OF DEF., DEFENSE PROGRAMS AND BUDGET OF JAPAN: OVERVIEW OF FY2023 BUDGET 34 (2022), https://www.mod.go.jp/en/d_act/d_budget/pdf/230330a.pdf [https://perma.cc/W9RG-64UA]. The document provides an explanation of AI-based accelerated decision making, stating that funds will be used to "[c]onduct research on technology to support commanders' decision-making into equipment by analyzing the course of action using AI to cope with the complex and fast changing combat situations." *Id.* at 40.

78. *See Australia Invests in AI Technologies to Build Defence Military Capability*, ARMY TECH. (Nov. 18, 2021), https://www.army-technology.com/news/australia-invests-ai-technologies/ [https://perma.cc/GC4D-KWV8].

79. *See* Masaya Kato, *Japan Steps Pp Deployment of Defense AI and Robots*, NIKKEI ASIA (Jan. 27, 2019), https://asia.nikkei.com/Politics/Japan-steps-up-deployment-of-defense-AI-and-robots.

80. Cai Hong, *Japan to Beef Up Deploying AI Technology in Military Defense*, CHINA DAILY (Feb. 12, 2019), https://www.chinadaily.com.cn/a/201902/12/WS5c6226caa3106c65c34e8dac.html [https://perma.cc/F7BL-RVW7].

assessments from its artificial intelligence."[81] Another shift in policy occurred in June 2023, when the Kishida government announced the release of the nation's first space security blueprint. The blueprint outlines the nation's new policies regarding space-based information systems to enhance the military's first strike or counterstrike capabilities. One of the central pillars of this blueprint is the use of AI to enhance space-based capabilities with the goal of increasing "the speed of information transmission by combining multiple small satellites and improve [] visual data interpretation technologies by using artificial intelligence."[82]

Australia is also making important strides in AI-based weapon procurement and development. The Australian Defence Force currently employs a number of AI-based systems, primarily in the field of autonomous weapons and vessels. One example is the Boeing MQ-28 Ghost Bat, an autonomous ariel vehicle developed by Boeing Australia. First launched in 2021, the vehicle operates through AI to act as a force multiplier for manned fighter aircraft by scouting for enemy planes, absorbing enemy fire, and providing critical resupply.[83] The Australian military has also begun to develop autonomous surface vessels and submarines powered by AI.[84]

The final element of Japan and Australia's national security-based strategies is leveraging their close ties to each other and the United States. Currently, Japan, Australia, and the United States are parties to the Quad, a four-member security forum with India. Recent talks have highlighted commitments among the Quad's members to enhance collaboration in the development of AI technologies to "help counter China's disruptive behavior in the region, particularly the country's malicious use of AI for surveillance, censorship, and misinformation."[85] Furthermore, Japan and

81. Inder Singh Bisht, *Japan Plans Armed Wingman Drone Development With U.S.: Report*, DEF. POST (June 7, 2022), https://www.thedefensepost.com/2022/06/07/japan-armed-wingman-drone/?expand_article=1 [https://perma.cc/J5Z3-UN8T].

82. *Japan Adopts Space Security Policy, Vows to Expand Defense Use*, KYODO NEWS (June 13, 2023), https://english.kyodonews.net/news/2023/06/caac42b9ada8-japan-adopts-space-security-policy-vows-to-expand-defense-use.html [https://perma.cc/HC7X-PZER].

83. *See* Thomas Newdick, *USAF Eyeing MQ-28 Ghost Bat for Next Gen Air Dominance Program*, THE WARZONE (Aug. 24, 2022, 6:10 PM), https://www.twz.com/usaf-might-buy-mq-28-ghost-bats-for-next-gen-air-dominance-program [https://perma.cc/4SQP-QXQR].

84. *See* Toby Walsh, *The Defence Review Fails to Address the Third Revolution in Warfare: Artificial Intelligence*, THE CONVERSATION (Apr. 28, 2023, 12:33 AM), https://theconversation.com/the-defence-review-fails-to-address-the-third-revolution-in-warfare-artificial-intelligence-204619 [https://perma.cc/WNJ4-LM4D].

85. Ngor Luong & Husanjot Chahal, *The Future of the Quad's Technology Cooperation Hangs in the Balance*, COUNCIL ON FOREIGN RELS. (June 14, 2022, 11:27 AM), https://www.cfr.org/blog/future-quads-technology-cooperation-hangs-balance [https://perma.cc/7YKU-2PY4].

Australia have begun to discuss bilateral cooperation in helping each other develop AI technologies for security and intelligence purposes.[86]

In terms of their respective relationships with the United States, both Japan and Australia have prioritized cross-border collaboration with the American government. In the case of Japan, Prime Minister Kishida is keen on deepening military ties with the United States, and sees AI as an important pillar of that policy. The Kishida government's rapid expansion of military spending in an effort to withstand Chinese aggression has left many believing that deeper ties with the United States is essential for regional security. Closer cooperation in AI development is seen as crucial, given the United States's immense advantages in AI production both within the U.S. military and the private sector.[87] The United States also appears to view Japan as an important partner in AI development for security purposes. The Biden Administration has released numerous press releases that discuss the importance of U.S.-Japan relations in the context of AI development.[88] What exactly this relationship will look like, however, is not entirely clear. There appears to be few concrete initiatives that have emerged between the two nations in terms of AI development. While the two have agreed to establish semiconductor research hub (that will presumably be used to develop chips necessary for AI processing),[89]

86. *See* Kana Inagaki & Nic Fildes, *Japan and Australia Set to Strengthen Military Intelligence Ties*, FIN. TIMES (Oct. 21, 2022), https://www.ft.com/content/37d6ddc7-589b-4e92-9851-3b4b139f02e4.

87. *See* Mikayla Easly, *Japan to Accelerate Integrated Deterrence with U.S. as Hedge Against China*, NAT'L DEF. MAG. (Feb. 18, 2022), https://www.nationaldefensemagazine.org/articles/2022/2/18/japan-seeks-to-accelerate-integrated-deterrence-with-us [https://perma.cc/NJ27-PHK9]; *see also* James L. Schoff et al., *A High-Tech Alliance: Challenges and Opportunities for U.S.-Japan Science and Technology Collaboration*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 29, 2021), https://carnegieendowment.org/2021/07/29/high-tech-alliance-challenges-and-opportunities-for-u.s.-japan-science-and-technology-collaboration-pub-85012 [https://perma.cc/CQ52-QL65].

88. *See*, *e.g.*, Press Release, White House Briefing Room, FACT SHEET: *The U.S.-Japan Competitiveness and Resilience (CoRe) Partnership* (May 23, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-the-u-s-japan-competitiveness-and-resilience-core-partnership/ [https://perma.cc/HTZ3-24SX]; Press Release, *U.S. Dep't of Def., Joint Statement of the U.S.-Japan Security Consultative Committee ("2+2")* (Jan. 6, 2022), https://www.defense.gov/News/Releases/Release/Article/2891314/joint-statement-of-the-us-japan-security-consultative-committee-22/ [https://perma.cc/QH26-4AWX]; Press Release, *U.S. Dep't of State, Reaffirming the Unbreakable U.S.-Japan Alliance* (Mar. 14, 2021), https://www.state.gov/reaffirming-the-unbreakable-u-s-japan-alliance/ [https://perma.cc/NHQ7-TKZU].

89. *See* Dashveenjit Kaur, *Japan, US Join Forces to Stay Ahead in the Semiconductor Race*, TECH HQ (Aug. 2, 2022), https://techhq.com/2022/08/semiconductor-chip-supply-chain-japan-us/ [https://perma.cc/4XW7-S84H].

it is not altogether apparent what sort of collaboration is planned for defense-related research and production.

Australia appears to have developed more concrete initiatives with the United States. The United States and Australia currently belong to a three-member security alliance with the United Kingdom known as AUKUS, which is considered one of the most consequential pacts in the Western Pacific. According to one analyst, "AUKUS is truly unique because of its exclusive focus on modernizing and enhancing the interoperability of the participants' military capabilities to deter and, if necessary, defeat China in a potential future conflict."[90] It is through AUKUS that a great deal of defense-related AI has been exchanged between the United States and Australia. For example, in April 2023 the United States, Australia, and United Kingdom jointly tested AI-powered drone swarms. These drone swarms contain immense potential as they can track and detect military targets, assist stealth aircraft, flood enemy radar, and analyze military targets to identify the best method of attack.[91] Furthermore, in 2022 AUKUS established a working group to research and develop joint AI capabilities, which "will provide critical enablers for future force capabilities, improving the speed and precision of decision-making processes to maintain a capability edge and defend against AI-enabled threats."[92] Outside of the AUKUS framework, Australia has taken on bilateral measures with the United States. One example can be found in Australia's 2023 Department of Defence budget, which highlights that the two nations signed a "Collaborative Aircraft Project Arrangement," which includes the development of the AI-powered MQ-28A Ghost Bat aircraft.[93]

90. Derek Grossman, *Why China Should Worry About Asia's Reaction to AUKUS*, FOREIGN POL'Y MAG. (Apr. 12, 2023, 11:51 AM), https://foreignpolicy.com/2023/04/12/aukus-china-indo-pacific-asia-submarines-geopolitics/ [https://perma.cc/P4GJ-JMN8].

91. Gabriel Honrada, *AUKUS Is Moving to Intelligent Drone Swarms*, ASIA TIMES (May 27, 2023), https://asiatimes.com/2023/05/aukus-moving-from-nuke-subs-to-ai-drone-swarms/ [https://perma.cc/Z2SH-4T8C].

92. Press Release, White House Briefing Room, FACT SHEET: *Implementation of the Australia-United Kingdom-United States Partnership (AUKUS)* (Apr. 5, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/ [https://perma.cc/7Q6G-9D8M].

93. *See* AUSTL. GOV'T: DEP'T OF DEF., PORTFOLIO BUDGET STATEMENTS 2023-24: DEFENCE PORTFOLIO 119 (2023), https://www.defence.gov.au/about/accessing-information/budgets/budget-2023-24 [https://perma.cc/NXH8-MG2E].

2. South Korea and Taiwan

Japan and Australia have undoubtedly emerged as two leaders in the Western Pacific's development of policies and laws aimed at developing AI for national security. Yet South Korea and Taiwan are also important players. South Korea and Taiwan's development of AI has differed from Australia and Japan in several respects, and it is in part due to differing security environments. Both face imminent threats of military activity within their borders—erratic and dangerous military behavior by North Korea in the case of South Korea and possible Chinese invasion in the case of Taiwan. It is out of this differing security environment that AI development in Taiwan and South Korea has taken on a certain degree of urgency. Both nations have made substantial investments in AI-based weaponry aimed at defending against potential invaders; both have relied heavily on the United States to provide weapons; and both have established laws and policies to develop AI research centers or workforces.

In the case of South Korea, the nation has placed the development of AI research centers at the core of its defense strategy. The first of these centers was created in 2018. Named the Korea Army Research Center for Future and Innovation, the center combines the research capabilities of the nation's largest defense company, Hanwha Systems, with the government's Korea Advanced Institute of Science and Technology. Specifically, the center is aimed at covering research in "AI-based command and decision systems, composite navigation algorithms for mega-scale unmanned undersea vehicles, AI-based smart aircraft training systems, and AI-based smart object tracking and recognition technology."[94] The South Korean Army also launched its Artificial Intelligence Research and Development Center in 2019 with the goal of building "the vision and concept for military applications of AI and to develop the next generation of combat power."[95] The reason for such aggressive investment in research? North Korea. As one group of scholars notes, these centers were driven in large part by South Korea's "ever impending need to securitize itself against its North Korean neighbor . . .

94. Rich Haridy, *South Korea Establishes Research Center to Develop Autonomous Weapons*, NEW ATLAS (Feb. 26, 2018), https://newatlas.com/korea-ai-weapons-military-kaist-hanwha/53576// [https://perma.cc/6B3H-UW6S].

95. Su Fei, *Military Developments in Artificial Intelligence and Their Impact on the Korean Peninsula*, *in* 2 IMPACT OF A.I. ON STRATEGIC STABILITY & NUCLEAR RISK 33, 33 (Lora Saalman ed., Stockholm Int'l Peace Rsch. Inst. 2019).

as both the public and private sectors are immediately threatened by any hostility from North Korea."[96]

In terms of developing AI-based weapons and defense systems, South Korea has made some of the heaviest investments of any nation in the Western Pacific. One area of note is cybersecurity. Researchers have noted that because North Korea frequently engages in widespread cyberattacks on South Korea, AI-based cyber defense systems will likely move "at a faster pace than other states."[97] And in fact, South Korea has already prioritized developing AI-based defenses. Its 2019 National Cybersecurity Strategy states that the nation will "[e]xpand the scope of detecting cyber attacks to enable real-time detection and blocking, and develop AI-based response technologies."[98] Furthermore, the Korea Internet and Security Agency has been using AI to develop measures to identify potential cyberattacks and detect vulnerabilities in critical networks.[99]

Outside of cybersecurity, Korea has developed further advances in defensive AI. In 2023, the South Korean Ministry of National Defense formalized its "Defense Innovation 4.0" plan. The plan is aimed at modernizing the South Korean military with the latest technological developments in order to adapt to new threats emerging from North Korea, and it focuses heavily on AI.[100] According to Vice Minister of National Defense Shin Beom-chul, one of the major developments in weapons technology under Defense 4.0 is the addition of more "AI-based drones and robots" to the military's arsenal, which will work to "reduce manpower while increasing combat efficiency."[101] The focus on AI-based

96. Lance Hunter et al., *A Lesser-Known Arms Race: The Military Application of Artificial Intelligence in Non-Major Power Developed States and the Implications for Global Security*, 3 INT'L J. SEC. STUD. & PRAC. 1, 22 (2023).

97. *Id.* at 23.

98. S. KOREA NAT'L SEC. OFF., NATIONAL CYBERSECURITY STRATEGY 16 (2019), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf [https://perma.cc/52ZV-SYBC].

99. *See* Fei, *supra* note 95, at 34-35.

100. *See* Sarah Kim, *Yoon Calls for 'Massive' Military Upgrades at Defense Committee Launch*, KOREA JOONGANG DAILY (May 11, 2023), https://koreajoongangdaily.joins.com/2023/05/11/national/defense/Korea-defense-innovation-committee-inauguration/20230511171857810.html [https://perma.cc/Y9LB-VAXA]; Dong Yon Kim, *North Korea's Grey Huddle: A Reverse Perspective of its Analog Military*, INST. FOR SEC. & DEV. POL'Y (Aug. 3, 2023), https://isdp.eu/wp-content/uploads/2023/08/Brief-Aug-3-North-Korea.pdf [https://perma.cc/5XEG-QFWG].

101. Felix Kim, *South Korea Counters North Korean Threats with AI-Based Drones, Robots*, INDO-PAC. DEF. F. (Apr. 13, 2023), https://ipdefenseforum.com/2023/04/south-korea-counters-north-korean-threats-with-ai-based-drones-robots/ [https://perma.cc/C22D-3FPF].

drones and robotics in Defense 4.0 is not surprising given that South Korea has sought to expand these fields for years. Because the nation currently faces an increasingly ageing population, the manpower of the Korean Armed Forces has substantially declined over recent years. In fact, experts predict that the current manpower total of 500,000 will be reduced to 400,000 by 2030.[102] Investment in AI presents a novel policy solution to this problem, as unmanned drones and robotics can help to provide critical defenses and replace lost soldiers and airmen. Beyond its ageing population, another motivation for Defense 4.0's AI investment—particularly in drone technology—is the fact that North Korean drones have begun to pose a serious threat. In December 2022, for example, North Korean surveillance drones infiltrated the South Korean airspace, generating headlines and alarm across the peninsula.[103]

Like South Korea, Taiwan has begun to rapidly expand its AI capabilities due to the ever-looming threat of military confrontation. Given that there is growing evidence that China's People's Liberation Army (PLA) will make widespread use of AI in a possible invasion of Taiwan,[104] defensive AI-technology has become essential for Taiwan's military. In fact, Taiwan's Ministry of National Defense has explicitly noted its concern regarding the rise of AI in the PLA. In its 2021 National Defense Report, the Ministry cautioned that China "has been applying AI in developing its unmanned systems, precision strike capabilities, war gaming, and Deepfake technologies, in order to greatly enhance its capabilities to conduct joint operations. The development could seriously impact the security in the Taiwan Strait and the region."[105]

To counter imminent threats from abroad, Taiwan has begun to invest in AI-based research and development. In 2018, for example, the government announced a $1.2 billion initiative to fund AI research in a

102. *See* Felix Kim, *South Korea Enhances Defense with Robotics, AI Systems*, INDO-PAC. DEF. F. (Sept. 17, 2022), https://ipdefenseforum.com/2022/09/south-korea-enhances-defense-with-robotics-ai-systems/ [https://perma.cc/J95U-S3MD].

103. *See* Kim, *supra* note 101.

104. *See*, *e.g.*, Gabriel Honrada, *Smart Deterrence: China's AI-Warfare Plan for Taiwan*, ASIA TIMES (Jan. 17, 2023), https://asiatimes.com/2023/01/smart-deterrence-chinas-ai-warfare-plan-for-taiwan/ [https://perma.cc/KJ6T-B2RC]; Koichiro Takagi, *New Tech, New Concepts: China's Plans for AI and Cognitive Warfare*, WAR ON THE ROCKS (Apr. 13, 2022), https://warontherocks.com/2022/04/new-tech-new-concepts-chinas-plans-for-ai-and-cognitive-warfare/ [https://perma.cc/7GTP-GHVK].

105. TAIWAN MINISTRY OF NAT'L DEF., NATIONAL DEFENSE REPORT 28 (2021), https://www.ustaiwandefense.com/tdnswp/wp-content/uploads/2021/11/Taiwan-National-Defense-Report-2021.pdf [https://perma.cc/NQ9Y-6ULY].

variety of areas, including national defense.[106] Yet Taiwan's approach to AI research and development for defensive purposes appears to differ from some of the other major actors in the Western Pacific in several respects. First, unlike South Korea, Japan, and Australia, Taiwan does not appear to have established separate AI research agencies within its defense ministry. There appears to be no equivalent of South Korea's Artificial Intelligence Research and Development Center or Australia's Defence Artificial Intelligence Centre. Second, Taiwan has invested in recruiting AI professionals from abroad to turbocharge AI development. In 2018, the government passed the "Act for the Recruitment and Employment of Foreign Professionals," which is in part designed to attract AI professionals from abroad to work in Taiwan and develop AI for a variety of means, including military purposes.[107] A series of amendments to the law in 2021 sought to further attract foreign professionals in AI, as the government relaxed work and residence permit regulations, and eased eligibility requirements for family members.[108] This is a unique element of Taiwan's attempt to foster development of defensive AI, as no other nation in the region seems to have crafted similar workforce-based legislation.

As with South Korea, Taiwan has begun to add AI-based weaponry to its arsenal to prepare for a potential future attack. And as with South Korea, Taiwan has placed a heavy premium on developing AI-manned drones. One such drone that has recently been added is the Albatross II UAV, which uses AI to engage in surveillance of enemy targets and to track naval movements. The drone is unique in that it can stay in the air for sixteen hours without needing refueling or rest, and can travel distances of up to 300 kilometers.[109] Outside of intelligence capabilities, Taiwan sees drones as an incredibly powerful tool in assisting ground forces in the event of an invasion by the PLA. One such class of drones is known as "loitering munitions," which are programmed by humans to attack specific targets but use AI to conduct the operation and evade enemy fire. These drones are seen as particularly useful in providing air

106. *See* SADAMASA OUE, ARTIFICIAL INTELLIGENCE AND IMPLICATIONS FOR SECURITY COOPERATION IN ASIA, *in* DEF. POL'Y & STRATEGIC DEV. 1, 15 (Fu-Kuo Liu et al., eds., World Sci. 2021).

107. *See* TAIWAN NAT'L SCI. & TECH. COUNCIL, TAIWAN AI-READINESS REPORT 33 (2022), https://digi.nstc.gov.tw/File/5AF024B4C7281A84/e761bee6-a38c-4d5b-8481-fc36b83b25d8?A=C [https://perma.cc/CSU9-SEFC].

108. *Id.* at 34.

109. *See* Eric Cheung, *Taiwan Unveils its New Combat and Surveillance Drones as China Threat Grows*, CNN (Mar. 14, 2023, 5:11 AM), https://www.cnn.com/2023/03/14/asia/taiwan-china-military-drones-unveiled-hnk-intl/index.html [https://perma.cc/S3UK-QK3F].

support to ground forces, thus supplanting the support role traditionally played by fighter jets and helicopters. According to Lee His-ming, Taiwan's former Chief of General Staff and Vice Minister of National Defense, these drones will be "elemental to Taiwan's military ability to deter a possible Chinese war of conquest."[110]

3. Other States

Australia, Japan, South Korea, and Taiwan have all taken important steps in developing AI for national security purposes. Each state has in some capacity used legal regimes and policymaking tools to invest in AI research and development, develop governmental agencies, and procure defensive and offensive military systems. Though the security situation of Australia and Japan differs from that of South Korea and Taiwan, all four states share similar characteristics: highly advanced economies, well-functioning governments and bureaucracies, relative domestic tranquility, strong private sector involvement in AI, and networks of highly active research universities.[111]

Beyond these four nations, however, the integration of AI into national defense has been limited at best. Some nations have made broad-based commitments to developing AI for national security purposes. For example, in its 2021 "National Strategy On R&D and Application of Artificial Intelligence," Vietnam's government set a goal of establishing a center within the Ministry of Defence for big data storage and high-level computing. The government also proposed using AI "in the intelligentization and modernization of equipment and weapons, in the development of operational plans, in national defence systems, system of prevention, handling and rapid response against cyber, biological, chemistry warfare."[112] The Philippines recently announced a joint

110. Maximilian Schreiner, *AI in War: How Artificial Intelligence Is Changing the Battlefield*, THE DECODER (Jan. 9, 2023), https://the-decoder.com/ai-in-war-how-artificial-intelligence-is-changing-the-battlefield/ [https://perma.cc/ZTZ3-Y9LL].

111. *See* Ryan Fedasiuk & Elliot Silverberg, *From Maritime Quad to Tech Quintet: Imagining South Korea's Role in the Indo-Pacific Security Architecture*, NAT'L BUREAU ASIAN RSCH. (June 28, 2022), https://www.nbr.org/publication/from-maritime-quad-to-tech-quintet-imagining-south-koreas-role-in-the-indo-pacific-security-architecture/ [https://perma.cc/PB9X-LCWN]; ANDREW IMBRIE ET AL., GEO. CTR. FOR SEC. & EMERGING TECH., AGILE ALLIANCES: HOW THE UNITED STATES AND ITS ALLIES CAN DELIVER A DEMOCRATIC WAY OF AI (Feb. 2022), https://cset.georgetown.edu/publication/agile-alliances/ [https://perma.cc/SJF4-TBUF].

112. *National Strategy On R&D and Application of Artificial Intelligence*, SOCIALIST REPUBLIC OF VIET NAM: GOV'T NEWS (Mar. 17, 2021, 10:12 AM), https://en.baochinhphu.vn/national-strategy-on-rd-and-application-of-artificial-intelligence-11140663.htm [https://perma.cc/3P5A-E7PA].

research effort between the nation's Space Agency and Department of National Defense to develop satellite technology powered by AI.[113] While these developments are encouraging, neither of these states seems to have produced broad-based plans with concrete details on how to integrate AI into defensive or offensive military capabilities. And in many other states, AI does not seem to play a factor at all in defense strategy. In August 2023, New Zealand released its National Security Strategy for 2023-2028. The document only references AI's effects in a descriptive manner, and does not articulate a vision on how AI might play a role in the nation's defense capabilities.[114]

There has been some movement in Singapore. Singapore launched a defense partnership with the United States in 2018, in which Singapore's Defence Science and Technology Agency collaborates with U.S. agencies responsible for AI development.[115] The Ministry of Defence launched a similar partnership with France's Ministry of the Armed Forces in 2023 with the goal of developing cyber defense-related AI.[116] And in 2022, Singapore announced the formation of a fourth military branch called "Digital and Intelligence Services," which operates a digital operations technology center staffed will experts in AI.[117] Yet given the fact that Singapore has one of the smallest populations among the Western Pacific nations[118] and a relatively modest number of active

113. *See* Jerome Siacor, *The Philippines Leverages Space Tech for National Defence*, OPEN GOV ASIA (Apr. 19, 2022), https://opengovasia.com/the-philippines-to-max-on-space-tech-to-exert-nations-sovereignty/ [https://perma.cc/KKN5-7WE4].

114. For example, the document states in its "Security Outlook" section: "We live in an era of disruption. Climate change poses an existential challenge, especially for our Pacific partners. Existing and emerging technologies like artificial intelligence (AI) provide opportunities, but also amplify threats from both countries and criminals." N.Z. GOV'T, NEW ZEALAND'S NATIONAL SECURITY STRATEGY: SECURE TOGETHER 4 (2023), https://www.dpmc.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf [https://perma.cc/T85K-VRV6].

115. *See* Prashanth Parameswaran, *What's in the New U.S.-Singapore Artificial Intelligence Defense Partnership?*, THE DIPLOMAT (July 1, 2019), https://thediplomat.com/2019/07/whats-in-the-new-us-singapore-artificial-intelligence-defense-partnership/.

116. Eileen Yu, *These Two Countries Are Teaming Up to Develop AI for Cybersecurity*, ZDNET (Apr. 24, 2023, 5:51 AM), https://www.zdnet.com/article/these-two-countries-are-teaming-up-to-develop-ai-for-cybersecurity/ [https://perma.cc/FD9Y-SXD2].

117. *See* Mike Yeo, *Singapore Unveils New Cyber-Focused Military Service*, DEF. NEWS (Nov. 2, 2022), https://www.defensenews.com/global/asia-pacific/2022/11/02/singapore-unveils-new-cyber-focused-military-service/ [https://perma.cc/MM5A-TA36].

118. Singapore's population currently stands at 5.64 million. *See Population Trends: Overview*, SING. GOV'T: NAT'L POPULATION & TALENT DIV., https://www.population.gov.sg/our-population/population-trends/overview/ [https://perma.cc/AC8R-ATAJ] (last updated May 21, 2024).

duty military personnel,[119] it is unlikely that the nation will be able to develop an expansive array of AI capabilities on the level seen in larger countries like Australia, Japan, South Korea, and Taiwan.

In sum, the current picture of AI development for military purposes in the Western Pacific is one that is heavily skewed towards high-income, high-population states. Those countries with few resources or manpower have largely taken limited (or no) steps towards integrating AI into their national security apparatuses. As discussed in the following Subpart, this is one of the major weaknesses for the region.

B. Current Weaknesses

The governments of the wealthy, populated states of the Western Pacific have made some important strides in the developing laws and policies regarding the use of AI for security purposes. However, those developments have been a mixed bag, as there are important gaps that leave these states quite vulnerable to rising threats from China and North Korea. For example, no nation has modeled China and produced a comprehensive regulatory framework aimed at curtailing malicious foreign AI. At the same time, the lack of law and policymaking for security-related AI outside of Australia, Japan, South Korea, and Taiwan leaves many middle-income or smaller states with limited means to deter or combat AI-based aggression. This section outlines, in broad strokes, the three major weaknesses facing the region's national security AI legal frameworks and policymaking efforts: (1) lack of adequate regulation; (2) insufficient spending and investment; and (3) failure to develop partnerships beyond the United States.

1. Regulatory Frameworks

One weakness facing the region is the lack of comprehensive regulatory regimes to place guardrails on AI. As outlined in Part I.A, China has established one of the most wide-ranging AI regulatory schemes, which is in-part targeted at stemming the national security risks posed by AI's growth. The rest of the Western Pacific, however, has failed to keep pace. Currently, the development of comprehensive legal frameworks specifically aimed at regulating AI among the major players in the Western Pacific is limited at best and virtually nonexistent in most

119. Singapore's total active duty military personnel stands at roughly 60,000. *See Armed Forces Personnel Total—Singapore*, WORLD BANK, https://data.worldbank.org/indicator/MS.MIL.TOTL.P1?locations=SG [https://perma.cc/7YVR-CXYL] (last visited May 24, 2024).

cases.[120] Some states have attempted to create broad-based AI regulation. South Korea's government, for example, proposed its first wide-ranging AI regulatory bill in early 2023. Yet the bill is primarily targeted at regulating health and safety, establishing ethical guidelines and intellectual property rights, and encouraging greater private development of AI. The bill does not seem to address serious national security issues.[121] Taiwan has also engaged in attempts to regulate AI, but has run into political hurdles and no pending legislation seems likely to be implemented into law in the immediate future.[122]

This lack of AI regulation on national security risks poses great danger to the region. As outlined earlier, there is growing fear that China and other malign actors may wish to introduce AI-based tools to engage in forms of "cognitive warfare," whereby disinformation is spread and discord sowed within states. AI regulation could help to mitigate this by restricting the types of foreign AI that may enter a foreign country or by placing strict security review protocols. Yet so far, little development has emerged on this issue across the Western Pacific.

2. AI Spending and Investment

Perhaps the greatest weakness facing the Western Pacific's security-related AI development is a fundamental policy failure: inadequate spending and investment. Part II.A of this Article outlined the many steps taken by the region's leading powers to leverage AI for military purposes. And while these advances have achieved promising outcomes, they only

120. Regarding Japan, Singapore, and Taiwan, *See* Keiji Tonomura et al., *Artificial Intelligence 2024 Comparisons*, CHAMBERS & PARTNERS, https://practiceguides.chambers.com/practice-guides/comparison/996/13358-13343-13354/21162-21163-21164-21165-21166-21167-21168-21169-21170-21171-21172-21173-21174-21175-21182-21187-21189 [https://perma.cc/5FLC-NSQD] (last updated May 28, 2024) (e.g., "Although the Cabinet Office has formulated a national strategy for AI, there are no cross-sectional and binding laws and regulations for AI in Japan."); regarding Australia, *see* Susannah Wilkinson & Julian Lincoln, *Momentum Is Building (Again) for AI Regulation in Australia*, HERBERT SMITH FREEHILLS (June 9, 2023), https://www.herbertsmithfreehills.com/insights/2023-06/momentum-is-building-again-for-ai-regulation-in-australia [https://perma.cc/E4YZ-KP6V] ("Currently, there is no AI-specific legislation in place in Australia.").

121. *See* Kim Yoo-chul, *Seoul's AI Legislation Could Be Game Changer*, KOREA TIMES (July 6, 2023), https://www.koreatimes.co.kr/www/tech/2024/02/129_354273.html [https://perma.cc/C2EN-FJ45]; Taeyoung Roh & Ji Eun Nam, *South Korea: Legislation on Artificial Intelligence to Make Significant Progress*, KIM & CHANG (Mar. 6, 2023), https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=26935 [https://perma.cc/956S-9H4W].

122. *See* Bryan Chuang & Jack Wu, *NSTC to Hold off on Basic AI Law Proposal Over Concerns That It May Hinder Innovation*, DIGITIMES ASIA (July 20, 2023), https://www.digitimes.com/news/a20230719PD203/ai-nstc-regulation-taiwan.html.

scratch the surface of what must be done to sufficiently secure these states from the threats posed, and harness the promises offered, by AI.

One area that has seen a lack of investment is research and development. While many states have created research centers, those centers are often vastly underfunded. For example, one expert argues that Australia's "Defence Artificial Intelligence Centre has been understaffed and under resourced"; as a result, each of the nation's military services has found it necessary to create its own respective AI program.[123] This has produced a diffused research hierarchy with no central guiding organization to coordinate research and collaboration.[124] Furthermore, while Japan is looking into developing a research center that is modeled on the United States's DARPA, there have been no concrete plans as of this writing to establish or fund such an enterprise.[125] Similarly, Taiwan lacks a major defense-based research center; and unlike Japan, there have been no reports to indicate that the country has any plans in the near-term to develop such a center.

Outside of the development formal centers, actual spending on AI-based research and development has been relatively limited. In its 2023 defense budget, for example, Japan earmarked spending for only one research project under the "Artificial Intelligence" heading, and spending for that program stands at only ¥4.3 (about $30 million).[126] It should be noted that in terms of research and development spending, South Korea has emerged as a leader. Its heavy (and relatively early) investment in its multiple AI research facilities is notable, and could serve as a guidepost for the rest of the region.

Another weakness in terms of spending and investment is the procurement and integration of AI-based weapons and defense systems. While there has been some progress in integrating AI-based technologies into the militaries of the region, this integration has lagged behind in many ways. As outlined in Part II.A, there has been investment among several of the region's powers in AI-based unmanned vehicles, especially in drone technology. Yet beyond this context, weapons acquisitions have been limited. In terms of cybersecurity, South Korea appears to be the only nation that has made major advances in using AI to defend against

123. Mick Ryan, *The Task Ahead for Rapid Capability Enhancement in Australian Defense*, CTR. FOR STRATEGIC & INT'L STUD. (Aug. 4, 2022), https://www.csis.org/analysis/task-ahead-rapid-capability-enhancement-australian-defense [https://perma.cc/5BV8-URKF].

124. *Id.*

125. *See supra* Part II.A.i.

126. DEFENSE PROGRAMS AND BUDGET OF JAPAN: OVERVIEW OF FY2023 BUDGET, *supra* note 77.

cyberattacks. This is concerning, especially given China's growing offensive cyber capabilities and concerns that China will employ cyberattacks in the event of a Taiwan invasion.[127] Another area that appears to be lagging is naval-related capabilities. Australia has expressed strong interest in integrating AI into the Royal Navy, and has taken steps to research autonomous flotillas and AI-assisted naval weapons and machinery.[128] South Korea has also taken steps to develop its naval capacities, as its Defense 4.0 strategy outlined a vision of heavily integrating AI into the Republic of Korea Navy.[129] Yet few other steps have been taken in the region to build-out AI capacities at sea. In fact, the Japan Maritime Self-Defense Force, which is one of the most powerful navies in the world,[130] does not appear to have made any significant investment in AI capabilities.

The two examples outlined above—cyber and naval—only scratch the surface of underinvestment in AI-based technology, as many other examples can be highlighted of an apparent lack of investment (such as AI-powered long-range artillery). Yet this underinvestment discussion so far has mainly focused on four states: Australia, Japan, South Korea, and Taiwan. And while those nations have only taken a patchwork approach to AI arms investment (meaning each nation seems to have invested in some areas but not others), they have at least made some investments in procuring and developing AI technologies for military purposes. The same cannot be said for the rest of the region. The limited or non-existent investment in AI from the rest of the region leaves open a gaping hole in regional security, as these states are increasingly vulnerable to the rising threat posed by AI from China and other malign actors.

127. *See* Emilio Iasiello, *Will China Replicate Russia's Cyber Offensives in a Taiwan Reunification?*, OODA LOOP (Feb. 15, 2022), https://www.oodaloop.com/archive/2022/02/15/will-china-replicate-russias-cyber-offensives-in-a-taiwan-reunification/ [https://perma.cc/MSQ8-XSJ3].

128. *See* Peter Dortmans et al., *Supporting the Royal Australian Navy's Strategy for Robotics and Autonomous Systems*, RAND CORP. (Sept. 14, 2021), https://www.rand.org/pubs/research_reports/RRA929-1.html [https://perma.cc/Q6RP-QT7L].

129. *See* Juho Lee, *South Korea Reveals New Unmanned 'Navy Sea GHOST' Concept*, U.S. NAVAL INST.: NEWS (Nov. 17, 2022, 2:02 PM), https://news.usni.org/2022/11/17/south-korea-reveals-new-unmanned-navy-sea-ghost-concept [https://perma.cc/BPF2-W4KT].

130. *See* Sinéad Baker, *The World's Most Powerful Navies in 2023, Ranked*, BUS. INSIDER (Aug. 6, 2023, 4:16 AM), https://www.businessinsider.com/most-powerful-navies-in-world-in-2023-ranked-ships-submarines-2023-8.

3. Lack of Partnerships Outside of, and Overdependence on, the United States

As outlined in Part II.A, many of the nations in the Western Pacific have established strong ties with the United States to develop AI capabilities. This has produced strong results in many instances. For example, the Royal Australian Air Force is partnering with the U.S. Air Force to produce a fleet of MQ-28 Ghost Bats.[131] And given that the United States is the global leader in AI, it is unsurprising that these nations have looked to the United States for research, development, and procurement partnerships. Yet this relationship with the United States faces two distinct problems. First, many of the region's nations have failed to construct healthy and productive AI-related relationships outside of the United States. Second, such close relations with the United States risk an overdependence on American military and technological innovation, which could pose a variety of challenges and ultimately place limits on technological innovation.

In a May 2022 report, Georgetown University's Center for Security and Emerging Technology analyzed AI-related collaboration within the Quad. The report states that each member of the Quad has specific AI capabilities "that could be leveraged for joint research opportunities."[132] For example, "Japan stands out in simulation and human-computer interaction," while Australia has strengths in "linguistics and theoretical computer science."[133] The report highlights that government policies could be implemented to encourage cross-border development, including allocating funding to support cross-border efforts, funding grants for joint research projects, establishing scholarships and fellowships for academics, and organizing conferences and workshops. Yet according to the report, these possibilities have largely failed to be realized. Instead, the report specifically notes that "[w]hile the United States collaborates extensively with Australia, India, and Japan on AI-related research, the latter three Indo-Pacific states collaborate little with one another."[134]

131. *See* Ryan Robertson, *Australia Wants to Build a Cauldron of Ghost Bat Drones with U.S.*, STRAIGHT ARROW NEWS (May 1, 2023), https://straightarrownews.com/cc/australia-wants-to-build-a-cauldron-of-ghost-bat-drones-with-us/ [https://perma.cc/LA7P-VVJV].

132. HUNSANJOT CHAHAL ET AL., GEO. CTR. FOR SEC. & EMERGING TECH., QUAD AI: ASSESSING AI-RELATED COLLABORATION BETWEEN THE UNITED STATES, AUSTRALIA, INDIA, AND JAPAN 1 (May 2022), https://cset.georgetown.edu/wp-content/uploads/Quad-AI.pdf [https://perma.cc/JML4-3S6C].

133. *Id.*

134. *Id.* at 2.

This document reflects the broader trend in the Western Pacific of failing to seek partnerships outside of the United States. While reports have noted that Japan and Australia have begun to discuss ways of cooperating together on defense-related AI,[135] there do not appear to be any concrete agreements as of yet. And while both South Korea and Australia noted in their 2021 Comprehensive Strategic Partnership that the two nations established a joint AI research project "to counter infectious disease,"[136] there does not appear to be any major cooperation in the national security realm. In many cases, AI cooperation does not even appear to factor into defense relationships with some of the major players in the region. Despite the fact that they are both highly developed democracies with strong ties to the United States, South Korea and Japan have long maintained testy relations due to historical tensions. The two nations have long had difficulties sharing even basic intelligence on North Korea—which poses a direct security threat to each nation—with each other.[137] It is thus unsurprising that little cooperation has developed between the two in the realm of AI for national security purposes. And in the case of Taiwan, given that no nation in the Western Pacific recognizes Taiwan as a sovereign state[138] and defense relationships are opaque at best,[139] there has predictably been little in the way of AI-based defense partnerships. Finally, given that most of the rest of the Western Pacific has failed to develop comprehensive AI programs for military

135. *See* Inagaki & Fildes, *supra* note 86.

136. AUSTL. GOV'T: DEPT. OF FOREIGN AFF. & TRADE, AUSTRALIA-REPUBLIC OF KOREA COMPREHENSIVE STRATEGIC PARTNERSHIP (2021), https://www.dfat.gov.au/geo/republic-of-korea/republic-korea-south-korea/australia-republic-korea-comprehensive-strategic-partnership [https://perma.cc/59FL-H2WN].

137. *See* Colin Clark, *South Korea and Japan Resume Intel Sharing Agreement, but Not All Problems Are Solved*, BREAKING DEF. (Apr. 17, 2023, 9:25 AM), https://breakingdefense.com/2023/04/south-korea-and-japan-resume-intel-sharing-agreement-but-not-all-problems-are-solved/ [https://perma.cc/H9ND-9UTA].

138. *See* Helen Davidson, *'Not About the Highest Bidder': The Countries Defying China to Stick with Taiwan*, THE GUARDIAN, (Apr. 3, 2023), https://www.theguardian.com/world/2023/apr/04/not-about-the-highest-bidder-the-countries-defying-china-to-stick-with-taiwan.

139. One report at the Global Taiwan Institute notes the following about Taiwan and Japan's defense relationship:

> The latest Japanese defense white paper identifies Taiwan as 'important for Japan's security and the stability of the international community.' . . . Yet, current legal authorities and established government-to-government channels do not effectively address how Japan can work with Taiwan, either bilaterally or with the United States, on a day-to-day basis.

Eric Chan & Wallace Gregson, *The Future of Taiwan-Japan Defense Cooperation*, GLOB. TAIWAN INST. (Aug. 10, 2022), https://globaltaiwan.org/2022/08/the-future-of-taiwan-japan-defense-cooperation/ [https://perma.cc/V6CF-JBWE].

capabilities, few partnerships have emerged with nations such as Vietnam, Indonesia, New Zealand, and the Philippines.

If the states of the Western Pacific do not develop more regional relationships, a great risk may emerge: overdependence on the United States for defense-related AI. Risk of overdependence on the United States beyond the AI context has become a major national security concern for many of the region's governments. Former Japanese Prime Minister Shinzo Abe was particularly concerned about his country's overdependence, and sought to expand Japan's independent military capabilities to reduce such dependence.[140] Experts in South Korea have warned that the nation is currently far too dependent on the United States for critical military technologies such as F-35 fighter jets.[141] These concerns can be extended to the AI realm as well. If the United States continues to be the only nation that the states of the Western Pacific engage with on AI, these states may find that they are dependent on the United States for AI tools. AI could in effect become the equivalent of South Korea's F-35 fighter jet quandary: crucial for national security, yet also mainly produced by a foreign power.

There is another risk that overdependence on the United might pose. Cooperation with solely the United States on national security-related AI necessarily limits the universe of foreign collaboration for domestic scientists. By not engaging with other regional actors on AI development, opportunities may be missed for cross-border development that could produce new and exciting technologies. Additionally, by solely engaging with the United States, defense-related researchers may be caught in trap whereby they develop only a limited framework for understanding AI's potential. Engagement with only the United States may mean that researchers limit their perspective on AI to their own national perspective and that of the United States. This, in turn, may produce a sclerotic research environment that fails to embrace new and different modes of thinking. Engagement outside of the United States would help to combat this, as it could introduce developers to entirely new methods and frameworks for understanding how AI can develop.

In summary, the current state of AI law and policy-making for national-security-related AI in the Western Pacific is a mixed picture. On

140. *See* Urs Schöttli, *Fear of China Brings Japan and South Korea Closer Together*, GIS (May 18, 2023), https://www.gisreportsonline.com/r/far-east-security/ [https://perma.cc/TG8K-UUNA].

141. *See* Jun Ji-hye, *Overdependence on US Weapons Weakens Military Independence*, KOREA TIMES (Sept. 29, 2015), https://www.koreatimes.co.kr/www/nation/2024/02/113_187687.html [https://perma.cc/BV3V-ZWWT].

the one hand, there has been a number of positive developments. Four nations—Australia, Japan, South Korea, and Taiwan—have taken some first steps to integrate AI into their militaries, and they have begun to develop policies and laws to foster AI research, development, and implementation. Though it occupies a rather small slice of the regional defense space, Singapore has also taken steps to integrate AI into its national security apparatus. Some developments in the region have occurred in a number of countries, as several states have embarked on tight AI-development relationships with the United States and have made investments in producing AI-powered drone technology. Other states have taken measures that are so far *sui generis*. Taiwan, for example, has passed a law aimed at recruiting foreigners to build AI in the defense space, while South Korea has invested heavily in building out AI for cyber defense capabilities. While these advances have been promising, there still remain major gaps within the region. No state thus far has developed a comprehensive regulatory regime to remedy the national security threats faced by unregulated AI. At the same time, spending and investment in AI by national defense ministries has been rather limited in some contexts and nonexistent in others. States like Vietnam and New Zealand have invested virtually no effort into developing defense-related AI, while spending in states like Australia and Japan still leaves much to be desired. Finally, the region risks overdependence on the United States for AI development as nations have largely failed to develop bilateral and multilateral agreements with other states in the Western Pacific.

C. Possibilities and Restraints on Future Law and Policymaking

How national-security-related law and policymaking develops in the Western Pacific over the next decade will be one of the most important developments for regional security. Should the region's nations embrace highly robust legal and policy regimes that promote AI development, AI could be used as a tool to deter Chinese aggression and ensure more a structurally sound balance of power in the region. Yet if AI policy and lawmaking falls by the wayside, the region risks facing a dominant China and dependence on U.S.-produced tools. This section of the article aims to highlight ways Western Pacific nations can develop laws and policies to enhance defense-related AI development. At the same time, this section will also highlight some of the legal barriers that could make expansion of national security AI more difficult. International humanitarian law (IHL), national legal constraints, and non-legal quandaries may place

barriers on the development of AI weaponry, international agreements regarding AI development, and the speed at which AI can advance.

IV. OPPORTUNITIES FOR DEVELOPMENT

Subpart II.B of this Article outlined three major areas of weakness facing the region's development of AI for national security: (1) lack of regulation; (2) inadequate spending and investment; and (3) lack of cross-border partnerships in AI development beyond the United States. This Part of the Article seeks to address ways in which these three weaknesses might be remedied. There are, of course, myriad avenues that the Western Pacific nations could take to tackle these problems. The suggestions below are merely some of the options on the table for these states. I base a number of my recommendations on strategies that are currently being implemented in other areas of the globe—namely, the European Union and Israel.

A. Regulatory Frameworks

As of this writing, China has developed the world's most comprehensive AI regulatory framework—one that takes specific aim at remedying the national security threats posed by the technology. Considering the threats posed by unregulated AI, it would be wise for the nations of the Western Pacific to follow suit and develop their own regimes. And while China has been the first nation to tackle AI regulation for national security needs, it need not be the model that the states of the Western Pacific follow.

Perhaps the best model that the states of the Western Pacific—especially those that are developed democracies—can follow is that of the European Union. Currently, the European Parliament is developing its much-publicized Artificial Intelligence Act, which promises to be one of the most comprehensive AI legal regimes in the world. This proposed law may be a better alternative to the Chinese model for the Western Pacific. The Artificial Intelligence Act contains regulations for "high risk" AI, which either outright bans such technologies or requires its producers to submit a "reasoned notification" to the relevant "national supervisory authorities" outlining why "their system does not pose a significant risk of harm to the health, safety, fundamental rights or the environment."[142]

142. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, EUR. PARL. DOC. P9_TA(2023)0236 (2023).

One of the high risk systems identified by the proposed law includes "AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda."[143] Furthermore, the law also requires AI systems to make users aware that "they are interacting with an AI system and require that content generated by AI, specifically that which generates images, audio, and video content that could be construed as authentic depiction of reality—such as a fake video depicting a person without their consent—be clearly labeled."[144] Finally, the law stresses that producers of high-risk AI must take measures—such as regular security patches—to ensure that those systems are not exploited by "adversarial attacks."[145]

Europe's proposed Artificial Intelligence Act provides an excellent national security framework from which the states of the Western Pacific can draw inspiration. The designation of certain categories of AI as "high-risk" allows greater scrutiny of technologies that could pose serious security risks. While the European law appears to focus heavily on AI that could be used to undermine elections and sow social discord, Western Pacific states could go even further. They could label even more categories as high risk, such as AI that has connections to critical national infrastructure (e.g., power grids). Furthermore, modifications could be made to the section focusing on protections against "adversarial attacks." States could require even more frequent security patches, and could insist that firms conduct regular tests to determine the degree of vulnerability their systems possess.

There are other regulatory options beyond the European Union example. One such option is trade controls. Much of the Western Pacific maintains deep AI ties with China as business partnerships and cross-border commercial activity have established enormous amounts of AI-related trade.[146] Given these close ties, and given the tense security situation with China and the rest of the region, it is incumbent upon the nations of the region to place strict guardrails on the import of Chinese

143. *Id.*

144. Faiza Patel & Ivey Dyson, *The Perils and Promise of AI Regulation*, JUST SEC. (July 26, 2023), https://www.justsecurity.org/87344/the-perils-and-promise-of-ai-regulation/ [https://perma.cc/T2CF-UELX].

145. EUR. PARL. DOC. P9_TA(2023)0236.

146. *See, e.g.*, NGOR LUONG ET AL., GEO. CTR. FOR SEC. & EMERGING TECH., CHINESE AI INVESTMENT AND COMMERCIAL ACTIVITY IN SOUTHEAST ASIA (Feb. 2023), https://cset.georgetown.edu/publication/chinese-ai-investment-and-commercial-activity-in-southeast-asia/ [https://perma.cc/SN49-A4RH].

AI. Import controls that specifically outline what types of AI may enter a particular country could help the prevent the introduction of malicious AI.

1. AI Spending and Investment

When compared to the United States and China, the Western Pacific's investment in defense-related AI technologies and research falls woefully behind. But this, of course, is not an entirely fair comparison. No state in Western Pacific maintains the economic, technological, or military might of either the United States and China, and it is thus unrealistic to assume that any of those nations could adopt strategies that run parallel with the world's two superpowers. However, other nations across the globe have shown that the procurement and development of AI for military purposes can be achieved by states with fewer resources at their disposals. Israel provides a good platform for understanding how Western Pacific governments can implement policies to establish robust defensive AI apparatuses within the constraints of more limited resources.

As a small nation (both geographically and numerically), Israel necessarily cannot make the same investments in AI as the United States and China. However, the Israel Defense Forces (IDF) has made vast strides in the development and procurement of AI-based systems. While much of the IDF's activity in the AI field is shrouded in secrecy,[147] recent reports show the immense scale of investment the military has put into AI. The chief of the IDF's operational data and applications unit announced recently that by 2028, half of the force's technologists—a number estimated in the thousands—will be devoted to working on AI.[148] In terms of AI's mergence with traditional weapons, the IDF has begun to use AI assistance in everything from tanks, to bombs, to even rifles.[149] Israel has also employs AI in more creative ways, such as using "AI to

147. The IDF refuses to even provide the exact amount it spends on AI funding. *See* Dan Williams, *Israel Aims to Be 'AI Superpower', Advance Autonomous Warfare*, REUTERS (May 22, 2023, 7:36 AM), https://www.reuters.com/world/middle-east/israel-aims-be-ai-superpower-advance-autonomous-warfare-2023-05-22/.

148. *See* Dan Williams, *From Rockets to Recruitment, Israel's Military Refocuses on AI*, REUTERS (June 13, 2023, 5:34 AM), https://www.reuters.com/business/aerospace-defense/rockets-recruitment-israels-military-refocuses-ai-2023-06-13/.

149. *See* Seth J. Frantzman, *Israel Unveils Artificial Intelligence Strategy for Armed Forces*, C4ISRNET (Feb. 11, 2022), https://www.c4isrnet.com/artificial-intelligence/2022/02/11/israel-unveils-artificial-intelligence-strategy-for-armed-forces/ [https://perma.cc/BRJ2-698X]; *see also* Seth J. Frantzman, *Israel's Carmel Program: Envisioning Armored Vehicles of the Future*, C4ISRNET (Aug. 5, 2019), https://www.c4isrnet.com/artificial-intelligence/2019/08/05/israels-carmel-program-envisioning-armored-vehicles-of-the-future/ [https://perma.cc/6XQY-WYU6].

assist [] offensive decision-making, for example to determine if a target is a military or a civilian one. In addition, some defensive tools are used to alert forces that they are under threat of a rocket or missile attack, or to aid in better safeguarding border movement."[150] Other advances include using AI to "select targets for air strikes and organize wartime logistics."[151] In terms of cyber defense, Israel is seen as a leader, and the Director of Shin Bet (Israel's internal security service) has stated that AI has seamlessly been incorporated into the service's systems and has helped to foil a number of cyberattacks.[152]

Israel's investment in national-security-related AI, while at times controversial,[153] is among the most substantial and cutting-edge in the world. This is due in large part to the government's active role in promoting pro-AI policies. For example, Israel's government released a strategy in 2022 to drastically overhaul the military's AI development, which included centralizing AI development into a single, unified agency.[154] All of this is due to a sustained effort by the government to transform Israel into a "superpower" for military-based AI.[155] The governments of the Western Pacific would perhaps be wise to take notes from Israel. Like Israel, many of the nations of the Western Pacific have some of the most advanced technological industrial bases, research centers, and companies.[156] And like Israel—which faces increasingly hostile tensions with nearby Iran—the states of the Western Pacific exist in a fragile security environment. For these reasons, the Western Pacific might look to Israel as a useful guide. At the same time, many of these

150. Tal Mimran & Lior Weinstein, *The IDF Introduces Artificial Intelligence to the Battlefield—A New Frontier?*, WEST POINT: LIEBER INST. (Mar. 1, 2023), https://lieber.westpoint.edu/idf-introduces-ai-battlefield-new-frontier/ [https://perma.cc/53HH-LWGQ].

151. Marissa Newman, *Israel Quietly Embeds AI Systems in Deadly Military Operations*, BLOOMBERG (July 16, 2023, 11:00 PM), https://www.bloomberg.com/news/articles/2023-07-16/israel-using-ai-systems-to-plan-deadly-military-operations#xj4y7vzkg.

152. *See* Peter Aitken & Yonat Friling, *Israel Embraces Cutting-Edge AI to Thwart Cyberattacks, Foil Terrorism*, FOX NEWS (June 28, 2023, 2:00 AM), https://www.foxnews.com/world/israel-embraces-cutting-edge-ai-thwart-cyberattacks-foil-terrorism [https://perma.cc/JJ64-WQJL].

153. *See* Mehul Reuben Das, *Uneasy Marriage: Israel Using AI to Conduct Airstrikes in Palestine as Ethical Questions Abound*, FIRSTPOST (July 17, 2023), https://www.firstpost.com/tech/world/israel-using-ai-to-conduct-airstrikes-in-palestine-as-ethical-questions-abound-12876372.html [https://perma.cc/CB2W-YMMR].

154. *See* Frantzman, *supra* note 149.

155. *See* Williams, *supra* note 147.

156. *See These Countries Have the Most Technological Expertise*, U.S. NEWS, https://www.usnews.com/news/best-countries/rankings/technological-expertise [https://perma.cc/JZU7-FT7V] (last visited May 24, 2024).

states actually have greater capacities to invest in military-based AI. Five nations in the Western Pacific—Japan, South Korea, Australia, Indonesia, and Taiwan—have larger national gross domestic products than Israel.[157] Three nations—South Korea, Japan, and Australia—also maintain larger defense budgets than Israel (with South Korea and Japan's budgets nearly eclipsing Israel's by a two-to-one ratio).[158]

In looking where to invest government resources, there are specific areas that the states of the Western Pacific should prioritize. One area concerns the security of national infrastructure. There is increasing concern among experts that AI tools may be used by either foreign adversaries or stateless actors to attack key infrastructures, including power grids, communication networks, internet connectivity, and transportation hubs.[159] Given that attacks on these types of infrastructure could seriously danger human and economic life, and could potentially weaken national defenses, it is imperative that more resources be devoted to defenses against these threats. Another area that should draw heavy investment is in naval technology. China's People' Liberation Army Navy (PLA Navy) is currently undergoing a massive expansion in ship production as the nation seeks to dominate the waters of the Western Pacific.[160] AI technology has begun to be integrated into the PLA Navy as technologists have used AI to accelerate ship production.[161] Given that future of the Western Pacific will be heavily driven by action on the seas, Western Pacific nations should make similar investments in naval AI technology. Not only could AI be used to increase ship production, but

157. *See GDP (current US$)*, WORLD BANK, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

158. *See The Top 15 Military Spenders, 2022*, STOCKHOLM INT'L PEACE RES. INST. (Apr. 2023), https://www.sipri.org/visualizations/2023/top-15-military-spenders-2022 [https://perma.cc/TA7H-242M].

159. *See* Márk Szabó, *Should the Cybersecurity World Prepare for AI-Based Critical Infrastructure Attacks?*, ESET (June 26, 2023), https://www.eset.com/blog/consumer/should-the-cybersecurity-world-prepare-for-ai-based-critical-infrastructure-attacks/ [https://perma.cc/RG53-24CQ]; Phil Laplante et al., *AI and Critical Systems: From Hype to Reality*, 53 COMPUTER 45 (2020), https://ieeexplore.ieee.org/document/9237327 [https://perma.cc/D6FY-UAYV].

160. *See* Sam LaGrone, *Pentagon: Chinese Navy to Expand to 400 Ships by 2025, Growth Focused on Surface Combatants*, U.S. NAVAL INST. NEWS (Nov. 29, 2022, 8:16 PM), https://news.usni.org/2022/11/29/pentagon-chinese-navy-to-expand-to-400-ships-by-2025-growth-focused-on-surface-combatants [https://perma.cc/UJ7K-EYZU].

161. *See* Gabriel Honrada, *AI Warship Designer Accelerating China's Naval Lead*, ASIA TIMES (Mar. 19, 2023), https://asiatimes.com/2023/03/ai-warship-designer-accelerating-chinas-naval-lead/ [https://perma.cc/RQY4-SASZ].

highly advanced AI could be used to degrade adversarial navies by making such weapons as anti-ship missiles more effective.[162]

Implementing policies that develop and procure AI technologies could help to reduce one of the great problems facing many Western Pacific militaries: falling population. There has been an abundance of literature regarding how declining population throughout the region has generated deep concerns over abilities to maintain sufficient numbers of active-duty troops.[163] AI could help to remedy this problem. Experts have noted that AI can be used to fill in some of the gaps created by smaller populations. One expert notes: "[n]ew technologies also will play an important role in how Japan and other states manage the effects of demographic change on their security strategies. Robotics and other unmanned systems, including artificial intelligence, may offer some offsets for shrinking populations."[164] Yet recognition of this possibility is not solely limited to academic researchers as defense officials themselves have highlighted the potential for AI to stem the risk from falling active-duty rosters. Satosi Morimoto, Japan's former Defense Minister, stated in 2018:

> [a]s Japan's population continues to dwindle, the 240,000-strong Self-Defense Forces will be cut to half its current size. . . . Each person will have to do twice as much as they currently do. So labor saving using AI, such as unmanned aerial vehicles and ships, is an absolute must.[165]

---

162. *See* John Keller, *Lockheed Martin to Build LRASM Anti-Ship Missiles with On-Board Sensors and Artificial Intelligence (AI)*, MIL. + AEROSPACE ELECS. (May 26, 2023), https://www.militaryaerospace.com/sensors/article/14294380/antiship-missiles-sensors-artificial-intelligence-ai.

163. *See, e.g.*, Helen Davidson, *Taiwan's Military Recruitment Pool Shrinking Due to Low Birthrate*, THE GUARDIAN (Oct. 4, 2022), https://www.theguardian.com/world/2022/oct/04/taiwan-military-recruitment-low-birthrate-chinese-invasion-threat; Chung Min Lee & Kathryn Botto, *Demographics and the Future of South Korea*, CARNEGIE ENDOWMENT FOR INT'L PEACE (June 29, 2021), https://carnegieendowment.org/posts/2021/06/demographics-and-the-future-of-south-korea?lang=en [https://perma.cc/PYU2-H7EF]; Robert D. Eldridge, *Japan's Changing Demographics and the Impact on Its Military*, 22 DEMOGRAPHICS, SOC. POL'Y, & ASIA 27-30 (2017).

164. Andrew Oros, *Japan's Demographic Shifts and Regional Security Challenges Ahead*, EAST-WEST CTR.: ASIA-PAC. BULL. (Aug. 26, 2020), https://www.eastwestcenter.org/publications/japan%E2%80%99s-demographic-shifts-and-regional-security-challenges-ahead [https://perma.cc/F5L3-FCZA].

165. *AI Bringing the Winds of Change to the Battlefield*, NHK WORLD—JAPAN (May 9, 2018), https://www3.nhk.or.jp/nhkworld/en/news/backstories/143/ [https://perma.cc/XJ3W-FKF9].

2. Establishing Strategic Partnerships

Much of the cross-border development of AI among Western Pacific nations is confined to transactions with the United States. While the United States is an important and useful partner in developing AI for national security purposes, Subpart II.B.iii of this Article highlights why partnerships solely with the United States present important national security risks. The states of the Western Pacific should begin to look to regional partners to develop AI. Given that global rankings of AI development place many nations in the Western Pacific (especially South Korea, Australia, Singapore, and Japan) among the world's leaders,[166] there is immense opportunity to leverage cross-border partnerships.

One of the advantages to leveraging cross-border relationships is that the development of AI across the region varies widely, with each state harboring great strengths and weak points. The strengths of one nation can help to complement the weaknesses of another, and vice-versa. For example, South Korea's private sector currently maintains the most robust investment in AI in the region, with an estimated $3.1 billion in investment in 2022 (nearly three times more than the next highest private sector investor in the region, Singapore).[167] States in the region with smaller degrees of private sector investment could implement policies that encourage collaboration with South Korean companies. Japan, by contrast, leads the region in terms of AI-powered industrial robot installations.[168] Countries could implement policies to foster collaboration with Japanese researchers to increase robotics development.

Developing relationships for defense-related AI development would also serve as a natural extension of already existing military collaborations. Many states in the region are currently engaged in either outright defensive alliances with each other or key partnerships that share critical technologies and defense information. Japan and Australia, for example, recently signed a Reciprocal Access Agreement that allows both nations to deploy fighter jets on each other's soil and commits both nations to joint military cooperation for defensive and humanitarian operations.[169] Other examples include South Korea and Singapore's 2022

166. *See Ground the Conversation About AI in Data*, STAN. UNI.: A.I. INDEX, https://aiindex.stanford.edu/ [https://perma.cc/3MNB-JDPB].

167. *See* AI INDEX STEERING COMM., INST. FOR HUMAN-CENTERED AI, STAN. UNIV., ARTIFICIAL INTELLIGENCE INDEX REPORT 2023 23 (2023), https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf [https://perma.cc/65YE-KB53].

168. *See id.*

169. *See* Press Release, Sen. the Hon. Penny Wong, Minister for Foreign Affairs, Australia and Japan deepen defence ties (Aug. 14, 2023), https://www.foreignminister.gov.au/minister/

agreement to cooperate on a wide range of defense-related activities and reserach[170] and the upgrading of South Korean and Australia's defense relationship to the "strategic partnership" level in 2021 (which resulted in the Republic of Korea Armed Forces participating in joint exercises with the Australian Defence Force).[171] Thus, strategic partnerships on AI would achieve the dual function of enhancing each nation's impressive AI advantages while also naturally integrating into already-existing regional defense pacts.

B. Limitations on Development

While there is great opportunity for the Western Pacific to expand its research and development of AI for national security purposes, the region faces a number of barriers that may limit the extent of this development. Many of these limitations are the result of legal protections in both international and domestic law. At the same time, non-legal constraints, such as budgetary economics, will also play a role in the shape of policy and lawmaking. This Subpart of the Article seeks to identify the main areas that will slow or prevent the development of certain national-security-related AI.

1. International Law

One of the factors that may hinder the development of AI for national security purposes is the limitations placed on military activities by international law. Currently, there are no international regulations that specifically govern the use of AI, let alone AI in the defense realm. However, general international legal principles may be invoked by governments, which in turn may make AI's application difficult in a military context.

Much of the law that is relevant for our purposes falls under international humanitarian law (IHL), which regulates war conduct. IHL is taken very seriously in the Western Pacific as many of the region's nations have repeatedly emphasized their respect and commitment to

penny-wong/media-release/australia-and-japan-deepen-defence-ties [https://perma.cc/ECG9-GZKX].

170. *See* Lim Min Zhang, *S'pore, South Korea Sign Upgraded Defence Pact on Sidelines of Shangri-La Dialogue*, STRAITS TIMES (June 11, 2022, 6:11 AM), https://www.straitstimes.com/singapore/spore-south-korea-sign-upgraded-defence-pact-on-sidelines-of-shangri-la-dialogue [https://perma.cc/5XX8-YSHA].

171. *See* Michael Smith, *Australia, Korea to Take Defence Ties to 'Next Level'*, AUSTRALIAN FIN. REV. (May 30, 2023, 12:12 PM), https://www.afr.com/world/asia/australia-korea-to-take-defence-ties-to-next-level-20230529-p5dca6 [https://perma.cc/92HJ-RZW7].

upholding the principles of IHL.[172] While IHL has not put specific guardrails on the application of AI for military purposes, there is growing literature suggesting that AI poses important questions under international law. These legal questions, combined with the high respect afforded to IHL by the Western Pacific, may make states more hesitant to fully encourage AI-based military developments.

One of the most prominent risks facing AI is that because AI-powered military systems do not contain human judgment, those systems may run afoul of the most basic tenants of IHL. IHL is currently comprised of four basic principles that a state must take into account before making a military decision: (1) military necessity (i.e., the means employed are strictly necessary for the completion of a military mission); (2) distinction/discrimination (i.e., distinguishing between military and civilian targets); (3) proportionality (i.e., the loss of life and property cannot be excessive when compared to the military gains achieved); and (4) unnecessary suffering (i.e., avoiding gratuitous violence).[173] Given the nature of these principles, these are highly subjective considerations. Yet scholars worry that because AI cannot make these subjective judgments, weapons based on AI might fail to abide by these principles. As one scholar notes:

> [The four principles] are all inherently anthropocentric principles that assume a subjective test, which a fully autonomous system cannot make. To illustrate this, one can again refer to the proportionality principle. IHL explicitly requires an assessment of the 'concrete and direct military advantage anticipated' and the excessiveness of the civilian harm. In other words, one has to appreciate what is reasonable and what is not. This balancing

172. *See*, *e.g.*, AUSTL. GOV'T: DEPT. OF FOREIGN AFF. & TRADE, INTERNATIONAL LAW, https://www.dfat.gov.au/international-relations/international-organisations/un/international-law [https://perma.cc/6WFP-Z8CW] ("Australia is dedicated to alleviating human suffering and protecting civilians in times of armed conflict through the application of international humanitarian law. We have been a strong supporter of the Geneva Conventions since we first signed them in 1950 and have ratified all three Additional Protocols."); Letter from the Delegation of the Republic of Korea to the United Nations, Status of the Protocols Additional to the Geneva Conventions of 1949 and relating to the protection of victims of armed conflicts (Oct. 10, 2016), https://www.un.org/en/ga/sixth/71/pdfs/statements/protocols/rok.pdf [https://perma.cc/RDH6-LE6R] ("[T]he Government of the Republic of Korea reaffirms its strong commitment to the implementation of international humanitarian law (IHL). . . . We, as States Parties of the Geneva Conventions, must uphold our firm commitments under IHL. Specifically, we should remain vigilant and put forward all means to ensure that parties to armed conflicts respect international humanitarian law.").

173. *See* David E. Graham, *The U.S. Employment of Unmanned Aerial Vehicles (UAVs): An Abandonment of Applicable International Norms*, 2 TEX. A&M L. REV. 675, 680 (2015).

> exercise is so subjectively loaded that it is difficult to imagine how an autonomous weapon system could ever evaluate it. It would only be possible if humans first determine precisely and "objectively" how much human suffering a given military advantage is worth. Not only is this almost impossible, it would also go directly against the core of IHL, which is to provide protection to those who do not or no longer participate in hostilities.[174]

Another element of IHL that may give pause to leaders in the Western Pacific is the doctrine of "constant care." The constant care doctrine developed out of an additional protocol to the Geneva Conventions, and it generally requires states to take precautionary measures to "spare the civilian population, civilians and civilian objects."[175] This involves, among other requirements, taking "all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[176] Scholar Shin-Shin Hua has outlined that AI-based weapons, such as autonomous weapons, run the risk of violating the constant care rule. She points out that because AI learning in weapons systems occurs outside of human purview, there may be an inherent unpredictability as to how these weapons function.[177] Specifically, because these weapons are able "to constantly 'learn' and adapt from experience," they may cause "unpredictable outcomes and inscrutable decision-making processes."[178] This unpredictability risks running afoul of IHL's constant care doctrine. By allowing these machines to make decisions free from human input, a risk develops that civilians may be targeted. Failure to take account of this risk would potentially violate IHL's requirement that states take precautionary measures by maintaining constant care.[179]

174. Matthias Cuypers, *Artificial Intelligence and International Humanitarian Law: Brothers in Arms or Rather the Opposite?*, KU LEUVEN (Apr. 5, 2023), https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/international-humanitarian-law [https://perma.cc/9MT7-33C5].

175. *Rule 15. Principles of Precautions in Attack*, ICRC DATABASE, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule15 [https://perma.cc/2TN4-4JKS].

176. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 57, June 8, 1977, 1125 U.N.T.S. 3, https://ihl-databases.icrc.org/assets/treaties/470-AP-I-EN.pdf [https://perma.cc/FDV4-XB7X].

177. Shin-Shin Hua, *Machine Learning Weapons and International Humanitarian Law: Rethinking Meaningful Control*, 51 GEO. J. INT'L L., 117, 137 (2019).

178. *Id.* at 120.

179. *Id.* at 128-30.

These two examples only scratch the surface of what has been a long-running debate on the intersection of IHL and AI-based weapons.[180] What is important for our purposes is to recognize how this debate might place limits on the development of defense-related AI. States throughout the Western Pacific may have great hesitancy to develop their AI capabilities given that such systems could violate international legal commitments. In fact, leaders throughout the region have already cautioned that their nations might restrict AI's use based on international law concerns. In Australia, top defense officials have pledged that the Australian Defence Force will not "deploy AI-equipped weapons if doing so breaches Australia's international law obligations."[181] Japan's Minister for Foreign Affairs cautioned in July 2023 that the "military use of AI . . . should be responsible, transparent and based on international law."[182] New Zealand has taken perhaps the most aggressive step in the region, calling for an international agreement to ban autonomous weapons systems in 2021.[183]

There is some evidence that certain states in the Western Pacific may not see IHL as that strong of an inhibitor to the development of military-based AI. For example, in 2023 Japan and Australia joined a statement authored by the United States that "asserts that the use of autonomous weapons systems should be deemed lawful as long as the states using them have taken effective measures to ensure that their use will not result in violations of international humanitarian law."[184] Additionally, a recent report noted that Australia has specifically avoided dealing with the legal

180. Good sources on this topic include: Afonso Seixas-Nunes, *Autonomous Weapons Systems and the Procedural Accountability Gap*, 46 BROOK. J. INT'L L. 421 (2021); Waseem Ahmad Qureshi, *The Changing Face of Warfare in the Hi-Tech World*, 49 SW. L. REV. 271 (2020); Alan L. Schuller, *At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law*, 8 HARV. NAT'L SEC. J. 379 (2017); Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347 (2016).

181. Andrew Tillett, *Military AI is More than Killer Robots*, AUSTRALIAN FIN. REV. (June 16, 2023, 3:26 PM), https://www.afr.com/politics/federal/military-ai-is-more-than-killer-robots-20230612-p5dfy4 [https://perma.cc/F2PN-9ZY8].

182. Statement by State Minister for Foreign Affairs of Japan Mr. TAKEI Shunsuke at the United Nation Security Council Briefing on "Artificial Intelligence: Opportunities and Risks for International Peace and Security", *Permanent Mission of Japan to the U.N.* (July 18, 2023), https://www.un.emb-japan.go.jp/itpr_en/takei071823.html [https://perma.cc/N7V9-LY94].

183. *See* Amy Cheng, *'Killer Robots' May Be Coming. New Zealand Wants to Stop Them.*, WASH. POST (Dec. 1, 2021, 4:33 AM), https://www.washingtonpost.com/world/2021/12/01/new-zealand-killer-robots-autonomous-weapons-law/.

184. Michael Klare, *Dueling Views on AI, Autonomous Weapons*, ARMS CONTROL ASS'N (Apr. 2023), https://www.armscontrol.org/act/2023-04/news/dueling-views-ai-autonomous-weapons [https://perma.cc/BDJ8-SWBV].

issues involving unmanned weapons systems and has instead pushed ahead with the development such weapons.[185]

2. Domestic Legal Concerns

While the intersection of IHL and AI has garnered much attention, there are also important constraints on AI development that may emerge from the laws of each country in the Western Pacific. In some cases, states have certain constitutional provisions, statutes, and regulations that may place impediments to the implementation of policies and laws aimed at growing defense-related AI.

Japan is a good example of how several existing constitutional and statutory standards may restrict development. One important example for defense-related AI involves Article 21 of Japan's constitution. Article 21 prohibits the government from violating "the secrecy of any means of communication."[186] This provision has been interpreted as aiming to prohibit "the government's access to internet communications and servers"—which could prove problematic in the national security context.[187] One commentator has noted that "Article 21 limits data collection to open-source information and prevents Japan's intelligence community to pursue cyber reconnaissance activities."[188] Another commentator has stated: "If it strictly applies [Article 21], Japan may not be able to engage with 'active cyber defense' (meaning cyber-attacks), nor share cybersecurity information with the U.S. or Australia."[189] This could prove particularly problematic for AI's integration into Japan's cyber defenses. If the government is not allowed to engage in "active cyber defense," it unlikely that the government would pursue strategies and policies to develop AI for cyber defense purposes. At the same time, this also harms Japan's capacity to engage in cross-border relationships to develop national security AI. If Japan is not engaged in building out AI

185. Matilda Byrne, *Australia is Lagging in its Approach to Autonomous Weapons*, AUSTL. INST. OF INT'L AFF. (July 6, 2023), https://www.internationalaffairs.org.au/australianoutlook/australia-is-lagging-in-its-approach-to-autonomous-weapons/ [https://perma.cc/U9P9-2RLY].

186. Nihonkoku Kenpō [Kenpō] [Constitution], art. 21, para. 2 (Japan).

187. *Id.*

188. Tomohiko Satake, *Japan-Australia Security Cooperation: Domestic Barriers to Deeper Ties*, STIMSON (Feb. 1, 2023), https://www.stimson.org/2023/japan-australia-security-cooperation-domestic-barriers-to-deeper-ties/ [https://perma.cc/FJL9-LTMD]; Alexandre Brans, *Japan's Evolving Cybersecurity Landscape: A Latecomer at a Crossroads*, ASIA POWER WATCH (July 21, 2023), https://asiapowerwatch.com/japans-evolving-cybersecurity-landscape-a-late-comer-at-a-crossroads/ [https://perma.cc/EMZ6-XUJ8].

189. Satake, *supra* note 188.

for cyber defense, there will be little incentive for other nations to partner with Japan in this sphere.[190]

Another area of concern for Japan is its State Secrecy Law. Passed in 2014, the "law provides for the protection of information in the categories of defense, diplomacy, counter-terrorism and counter-espionage" by allowing the government to prevent release of documents related to those categories.[191] However, the law does not specifically carve out protections for sensitive technologies. This has led some to worry that this may make other nations extremely hesitant to share sensitive national security technologies—such as AI—with Japan for fear that the secrecy of these systems might be compromised.[192] This gap in the State Secrecy Law is yet another example of how Japan's domestic laws may hinder cross-border collaboration over military-based AI.

In some cases, nations have established internal regulations that could restrict the development and deployment of AI in a military context. For example, internal codes at the Australian Department of Defence give military commanders the authority to employ AI, but also insist that these commanders have the responsibility "to ensure the pursuit of [the commander's] goals is ethical and lawful. There are no exceptions."[193] In abiding by these rules, military commanders might be hesitant to utilize AI for fear of violating ethical codes and guidelines. This is especially

190. It should be noted that despite the restrictions placed by Article 21, Japan does still seem to be building out cybersecurity capabilities. However, this development is shrouded by the threat that Article 21 may emerge as a legal liability at some point and cause serious headaches for military and intelligence officials. *See* Naoki Matsuyama, *Government to Add 'Active Cyberdefense' in Security Policy*, ASAHI SHIMBUN (Dec. 6, 2022), https://www.asahi.com/ajw/articles/14785897 [https://perma.cc/N4GH-G7T4] ("If a possible cyberattack is detected, the government is considering infiltrating the potential attacker's system or server and neutralizing the prospective attack, or launching counterattacks. However, such measures could violate Article 21 of the Constitution, which protects the secrecy of communications."); *see also* Scott Foster, *Japan's Cyber-Samurai Moving Out of the Shadows*, ASIA TIMES (Dec. 20, 2022), https://asiatimes.com/2022/12/japans-cyber-samurai-moving-out-of-the-shadows/ [https://perma.cc/LJ7V-EF6H].

191. Mina Pollmann, *Japan's Troubling State Secrets Law Takes Effect*, THE DIPLOMAT (Dec. 18, 2014), https://thediplomat.com/2014/12/japans-troubling-state-secrets-law-takes-effect/ [https://perma.cc/GG8L-S2ZF].

192. *See* Satake, *supra* note 188 ("Japan also needs to strengthen its security clearance system. Japan's secrecy law, which came into force in 2014, prohibits the leak of information in defense, diplomacy, espionage, and terrorism but does not cover other areas such as technologies. This makes it impossible for other countries, including Australia, to share sensitive information with Japan in areas like emerging technologies.").

193. S. KATE DEVITT & DAMIAN COPELAND, AI GOVERNANCE FOR NATIONAL SECURITY AND DEFENCE: ASSESSING MILITARY AI STRATEGIC PERSPECTIVES 26 (M. Raska et al., eds) (forthcoming).

worrying given that the ethical standards for AI are rather opaque—in fact, Australia has yet to even adopt an ethics framework for military use of AI.[194]

But perhaps the biggest legal hurdle to the development of AI for military purposes is not the laws that are on the books, but rather the absence of legal regimes. As outlined previously, Western Pacific nations have lagged in the development of a comprehensive AI regulatory scheme. But beyond this, Western Pacific nations have lagged behind in the development of any laws that even touch upon the topic of AI. A 2023 report by Stanford University totaled the number of "AI-related bills passed into law" across the globe between 2016 and 2022.[195] Among the fourteen top nations listed in the report, only three came from the Western Pacific: South Korea (ranked ninth), the Philippines (ranked tenth), and Japan (ranked fourteenth).[196] This lack of legal guidance or clarification may make AI developers wary about developing AI for national security projects. Without a legal framework to guide or sanction development, national-security-related agencies may be wary about implementing policies encouraging AI research, acquisition, or implementation.

3. Beyond Law: Other Practical Concerns

While law (or the lack thereof) may impose constraints on the development of national security-related AI, there are other factors that could play an even more important role. Perhaps the factor that may be most challenging to law and policymakers is the court of public opinion.

In a number of states throughout the Western Pacific, large sectors of the public oppose the development of AI in the military context. A 2019 poll by Ipsos put this into stark perspective. The poll asked respondents across the globe, "How do you feel about the use of [] lethal autonomous weapons systems in war?"[197] The response across the Western Pacific was unambiguous: respondents overwhelmingly opposed such weapons. In South Korea, 15% supported the use, while 74% opposed; in Australia, 15% supported and 59% opposed; and in Japan, 14% supported and 48% opposed.[198] A follow-up poll in 2021 found results had changed little in the intervening two years: in South

194. *Id.* at 28.

195. ARTIFICIAL INTELLIGENCE INDEX REPORT 2023, *supra* note 167, at ch.6.

196. *Id.*

197. Chris Deeney, *Six in Ten (61%) Respondents Across 26 Countries Oppose the Use of Lethal Autonomous Weapons Systems*, IPSOS (Jan. 22, 2019), https://www.ipsos.com/en-us/news-polls/human-rights-watch-six-in-ten-oppose-autonomous-weapons.

198. *Id.*

Korea, 19% supported and 65% opposed; in Australia, 19% supported and 64% opposed; and in Japan, 12% supported and 59% opposed.[199] Additionally, a 2023 study found that with regards to the use of AI in weapons, Japanese respondents were extremely concerned about the ethical, social, and legal ramifications of such devices. In fact, the study found that when compared to American or German respondents, Japanese participants were far more worried about AI-based weaponry.[200]

With numbers like these, leaders throughout the Western Pacific might be hesitant to foster policies and laws that encourage the development of AI for military means. Given that many of the states in the region are democracies, elected officials may feel pressure from their constituencies to avoid establishing pro-AI laws. Granted, the aforementioned studies focus exclusively on the development of AI weaponry, and does not assess how the public might feel about AI used outside of the weapons context (such as cyber defense).

Policymakers may also face barriers due to the unique nature of AI. One area this can best be seen is in the context of developing AI partnerships with other states in the region. While this article has argued that such partnerships should be pursued, there are concerns that the specific nature of AI may make such relationships difficult. Generally speaking, states recognize that there are inherent risks that might emerge from sharing sensitive information with foreign leaders. The fear is that once information is transmitted from one country to another, the transmitting country loses control over that information, and the receiving country may be reckless with its use of that information. To combat these risks, many states currently have restrictions (either through law or internal defense ministry guidelines) that restrict the kind of information that can be shared with international defense partners. One such control involves only sharing finalized intelligence products (e.g., reports) with defense partners but omitting the underlying data that support those reports. The trouble with AI is that its success is often dependent on that underlying raw data; and without that data, an AI system may not be able to function in an optimal manner. But as one expert notes, this data "can expose precise capabilities and shortcomings of a state's intelligence systems," and thus "decision-makers may be hesitant to share it—especially in the large quantities needed to develop and run many AI-

199. *Global Survey Highlights Continued Opposition to Fully Autonomous Weapons*, IPSOS (Feb. 2, 2021), https://www.ipsos.com/en-us/global-survey-highlights-continued-opposition-fully-autonomous-weapons.

200. Yuko Ikkatai et al., *Segmentation of Ethics, Legal, and Social Issues (ELSI) Related to AI in Japan, the United States, and Germany*, 3 AI & ETHICS 827, 838-40 (2023).

enabled systems."[201] Thus, with concerns like these, policymakers may be wary of developing deep AI collaborations in the national security sphere.

A final consideration that may limit the development of AI policies is a practical one: finances. This Article has encouraged large-scale investment in AI-related technologies, relationships, and research. That, of course, costs money—a lot of it. Many nations in the region, however, face serious budgetary limitations that limit their capacity to make deep investments. The wealthiest states in the region in terms of total GDP are Japan and South Korea. Yet both nations currently face ageing populations,[202] bloated national debts,[203] and high deficits.[204] The capacity of these states to make enormous investments in AI will necessarily be limited by these factors. Furthermore, many of the region's less-wealthy states, like the Philippines and Indonesia, currently have only modest defense budgets. The Philippines currently spends $4 billion on defense, while Indonesia spends $9 billion; by contrast Japan and South Korea each spend $46 billion.[205] It may simply be unrealistic to expect these nations to make major investments in AI with the limited funds at their disposal.

V. CONCLUSION

The emergence of AI has produced a new and complicated national security landscape for the Western Pacific. The region is currently locked between two rival superpowers—the United States and China—who have both made heavy investments in AI for military and defense purposes. At the same time, fears are growing that China and other actors (e.g., North

201. Erik Lin-Greenberg, *Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making*, 3 TEX. NAT'L SEC. REV. 56, 65 (2020).

202. *See* Claire Moses, *Aging Societies*, N.Y. TIMES (Feb. 19, 2023), https://www.nytimes.com/2023/02/19/briefing/asia-aging-popupulation.html.

203. *See* Leika Kihara & Tetsushi Kajimoto, *Japan's Debt Time Bomb to Complicate BOJ Exit Path*, REUTERS (Feb. 10, 2023, 6:15 AM), https://www.reuters.com/markets/asia/japans-debt-time-bomb-complicate-boj-exit-path-2023-02-10/; Yonhap, *S. Korea's Fiscal Deficit Expands On-Year in April*, KOREA HERALD (June 15, 2023), https://www.koreaherald.com/view.php?ud=20230615000251 [https://perma.cc/JVV6-BV8L].

204. Mariko Kodaki, *Japan Lags Behind U.S., U.K. in Curbing Pandemic Deficits*, NIKKEI ASIA (Mar. 29, 2023), https://asia.nikkei.com/Economy/Japan-lags-behind-U.S.-U.K.-in-curbing-pandemic-deficits2; Im Eun-byel, *Mounting National Debt Erodes S. Korea's Competitiveness: Report*, KOREA HERALD (June 20, 2023), https://www.koreaherald.com/view.php?ud=20230620000622 [https://perma.cc/D4MJ-4DFD].

205. *See Military Spending by Country*, WISEVOTER https://wisevoter.com/country-rankings/military-spending-by-country/ [https://perma.cc/CWJ7-RB5E] (last visited May 24, 2024).

Korea and stateless actors) may use AI to either develop cyber weapons or enhance the capabilities of already existing weapons systems. This is especially concerning in the case of Taiwan, where fears are growing that China may use AI-based weaponry in a possible future invasion of the island state.

In the wake of these threats, several nations in the region have begun to engage in law and policymaking that encourages the development of national security-related AI. However, these developments have largely been confined to a few states—namely Australia, Japan, South Korea, and Taiwan. And even among these nations, development has been lagging. For example, these states have yet to develop comprehensive regulatory regimes or make the necessary financial investment to truly maximize AI's potential or to reduce AI's risk. In order to protect themselves from the growing risk of China and other malign actors, these states must change their approach to national-security-related AI. Creating a strong regulatory framework, investing in research and development, and establishing bilateral and multilateral regional partnerships are all important steps that can be taken to put these nations on strong footing. Failure to take these steps may leave these nations highly vulnerable, and may result in an overdependence on the United States for AI technology.