

# THE US, INDO-PACIFIC, AI AND EMERGING SECURITY TECHNOLOGIES

*James Johnson*

## **Introduction**

This chapter considers US thinking and approaches to emerging technologies in the Indo-Pacific. It explores the intensity of the strategic competition – especially the role and presence of China – playing out within a broad range of Artificial Intelligence (AI) and other emerging security technologies in the region, including cyberspace, semi-conductors, 5G networks, autonomy and robotics, quantum computing, and big data analytics, to name a few.<sup>1</sup> It describes how great power competition is mounting within several dual-use high-tech fields, why these innovations are considered by Washington to be strategically vital, and how (and to what end) the US is responding to the perceived challenge posed by China to its technological hegemony.

The chapter uses International Relations (IR) concepts concerned with the nature and distribution of power within the international system, as a lens to view the shifting great power dynamics in AI and related emerging security technologies in the Indo-Pacific region. The current academic literature and debate on these issue have generally focused more broadly on the role of technology in international security, and more recently, debates have considered the intersection between emerging technology, rising powers, and shifts in the balance of power (Geist and Lohn, 2018; Gilli and Gilli, 2019; Horowitz, 2018; and Kennedy and Lim, 2017).

What have been the most important developments up to the present day in Washington's technology strategies in the Indo-Pacific? What AI capabilities does the US have in the region today? Will the increasingly competitive US-China relationship dominate world politics creating a new two-bipolar world order, as opposed to a multipolar one? (Boulanin, 2019; Geist and Lohn, 2018; Ayoub and Payne, 2016; Technology for Global Security, 2019; Johnson, 2019c). This chapter is an attempt to acquire greater insight into these questions, which have important implications for US-China relations and the future security landscape of the Indo-Pacific more broadly.

The chapter argues that the strategic competition playing out within a broad range AI and other emerging security technologies, will likely *narrow* the technological gap separating great military powers (notably the United States and China), and to a lesser extent,

other technically advanced small-medium powers in the Indo-Pacific such as South Korea, Singapore, and Japan. The chapter builds on the growing body of literature that reinforces the perception in the US that China's pursuit of AI and other emerging security technologies will threaten the unassailable first-mover advantage that the US has in a range of dual-use (with both commercial and military application) emerging security technology (Boulanin, 2019; Johnson, 2019a; Johnson, 2019c; Johnson, 2021; Horowitz, 2018; Moore, 2017; Allen and Chan, 2017).

The chapter proceeds as follows. First, it summarises the responses by US decision-makers and analysts to the debate about US decline and the rise of the narrative of an imminent shift in the distribution of power in the world order. This grand strategic overview will be contextualized with particular reference to the relative decline of the United States vis-à-vis China, and the implications of the US being displaced as the Indo-Pacific and global hegemon. It then sets up the debate over rapid advances and proliferation of emerging security technology, through an exploration of those that view harnessing these capabilities as a central aspect of efforts to maintain Washington's hegemony (or dominance) in the Indo-Pacific region. Next, it examines the perception of the rise of a bipolar (or two-power) order divided between Washington and Beijing. The chapter closes with commentary on the nature and potential implications of an arms race in emerging security technology between the US and its strategic rivals in the Indo-Pacific – especially China.

### **Emerging Challenges to US Technological Leadership in the Indo-Pacific**

In the post-Cold War era, a preoccupation with US policymakers and analysts has been the nature and implications of US hegemony. This discourse has centered on two key questions: How long will unipolarity last? Also, is the pursuit of hegemony a viable or worthwhile strategic objective for the United States to pursue? The preservation of the US liberal hegemonic role has been the overarching grand strategic goal of every post-Cold War administration from George H. W. Bush to Barack Obama (Layne, 2012 p. 2). The analysis that follows uses AI and emerging security technologies as a lens to explore how the US is positioning itself vis-à-vis the Indo-Pacific preparing for bipolarity with China or reluctantly accepting a multipolar order in the Indo-Pacific?

World leaders have been quick to recognize the transformative potential of AI-related technology as a critical component of national security (Work, 2015). In large part driven by the perceived challenges posed by rising revisionist and dissatisfied powers – especially China and Russia (US Department of Defense, 2017). In 2016 The US Department of Defense (DoD) released a 'National Artificial Intelligence Research and Development Strategic Plan' – one of a series of studies on AI machine learning, which was updated in 2019 – on the potential for AI to reinvigorate US military dominance (US Department of Defense, 2016; White House, 2019). In the context of managing the potential flashpoints in the Taiwan Straits, the South China Seas, and Ukraine, then-US Secretary of Defense Ashton Carter stated that Russia and China are the United States' "most stressing competitors" and continue to "advance military systems that seek to threaten our [US] advantages in specific areas" [including AI] and in "ways of war that seek to achieve their objectives rapidly, before, they hope, we [the US] can respond" (US Department of Defense, 2016). In a similar vein, the recent summary of the DoD's debut AI strategy stated that "China and Russia are making significant investments in AI for military purposes" that "threaten to erode our [US] technological and operational advantages." In response, the US must "adopt [military-use] AI to maintain its strategic position, prevail on

future battlefields, and safeguard this [i.e., US-led] order” (US Department of Defense, 2019a – emphasis added).

China and Russia have both developed a range of military-use AI technologies as part of a broader strategic effort to simultaneously exploit perceived US military vulnerabilities and reduce their own. In a quest to become a “science and technology superpower,” and catalyzed by AlphaGo’s victory (or China’s ‘Sputnik moment’), Beijing launched a national-level AI-innovation agenda for “civil-military fusion” – or US Defense Advanced Research Projects Agency (DARPA) with Chinese characteristics (State Council Information Office, 2017). Similarly, the Russian private sector has also benefitted from state-directed support of human capital development and early investment in advanced technologies, in a broader effort to substitute its continued dependence upon Western technology with indigenous technologies, and despite Russia’s weak start-up culture. In short, national-level objectives and initiatives demonstrate recognition by great military powers of the potential military-technological transformative potential of AI for national security and to strategic stability between great military powers (Johnson, 2020a, 2020b).

US analysts and policymakers have suggested a range of possible responses to these emerging security threats to preserve US technological leadership, which harnesses US natural advantages to pushback against the rising great military powers in the multipolar order (Hadley and Nathan, 2017; Work and Brimley, 2014; Gesit and Lohn, 2018; White House, 2019). First, the DoD should fund and lead AI-simulated war games or creative thinking exercises, to investigate existing and new security scenarios involving disruptive AI innovations. Second, the US needs to leverage its world-class think-tank community, academics, AI experts, computer scientists, and strategic thinkers to assess the implications of AI for a range of security scenarios and devise a strategic agenda to meet these challenges. Third, the US should prioritize DoD AI-based R&D to leverage the potential low-cost force multiplier advantages of AI technologies (i.e., autonomy and robotics), and to mitigate potential vulnerabilities and risks. Fifth, the US national security policy-making community (e.g., DARPA, the US Intelligence Advanced Research Projects Activity (IARPA), Defense Innovation Board (DIB); the Office of Naval Research (ONR); and the National Science Foundation (NSF)) should seek increased funding for AI-related research to combat the competition for talent and information in AI, actively support university programs to ensure the US retains its relative talent pool advantages – in particular vis-à-vis China. Finally, the Pentagon should fund additional R&D in reliable fail-safe and safety technology for AI-systems – especially military AI applications and tools (Hadley and Nathan, 2017).

### Washington’s New Sputnik Moment?

As AI military applications have grown in scale, sophistication, and lethality, many in the US defense community have become increasingly alarmed about the implications of this trend for international competition and national security (Hadley and Nathan, 2017 p. 17). In his opening comments at ‘The Dawn of AI’ hearing, Senator Ted Cruz stated, “ceding leadership in developing artificial intelligence to China, Russia, and other foreign governments will not only place the United States at a technological disadvantage, but it could have *grave implications for national security*” (Hadley and Nathan, 2017 p. 17). Similarly, Director of US National Intelligence Daniel Coates recently opined, “the implications of our adversaries’ abilities to use AI are *potentially profound and broad*” (ibid. p. 17, emphasis added).

Given the anticipated national security value China and Russia in particular attach to dual-use (i.e., military and civilian uses) AI-related technologies – notably autonomy and robotics,

quantum communications, and 5G networks discussed below – several defense analysts have characterized the exorable pace and magnitude of emerging security technologies (especially AI) as a ‘Sputnik moment’. This in turn might portend a military revolution by triggering an arms race in emerging security technologies and changing the character (or perhaps nature) of warfare. Emerging security technologies are, however, only one facet of a broader trend towards increasing the speed of modern (conventional and nuclear) war, and shortening the decision-making timeframe, associated with advances in weapon systems such as cyber-attacks, direct-energy weapons, quantum communications, anti-satellite weapons, and hypersonic missile technology (Wilkening, 2019; Johnson, 2019b; Johnson, 2021; Acton, 2013). These trends could lead to arms race instability between great powers – China, Russia, and the United States – in the Indo-Pacific region as rival states attempt to modernize their capabilities to reduce their perceived vulnerabilities (Schelling and Halperin, 1975; Johnson, 2020c).

Evidence of exponentially accelerated competition – in research, adoption, and deployment – of emerging security technologies (i.e., 5G networks, IoT, robotics and autonomy, additive manufacturing, and quantum computing), does not *necessarily* mean an ‘arms race’ is taking place. Instead, framing great power competition (especially US–China) in this way risks the adoption of operational concepts and doctrine that increases the likelihood of arms racing spirals and warfare (Roff, 2019 pp. 1–5). According to the DoD’s recently established Joint Artificial Intelligence Center (JAIC) former head Lt. General Jack Shanahan, “its strategic competition, *not an arms race*. They’re [China] going to keep doing what we’re doing; we [the US] acknowledge that.” Shanahan added: “What I don’t want to see is a future where our potential adversaries [China] have a fully AI-enabled force, and we [the US] do not” (Office of the Secretary of Defense, US Department of Defense, 2019a).

In response to a growing sense of consternation within the US defense community, the Pentagon has authored several AI-related programs and initiatives designed to protect US superiority on today’s digitized battlefield (e.g., Project Maven, DARPA’s ‘AI Next Campaign,’ the establishment of the JAIC, and the DoD’s ‘Artificial Intelligence Strategy’). Taken together, these initiatives demonstrate the perceived gravity of the threat posed to US national security from near-peer states’ (notably China and Russia) pursuit of emerging security technologies like AI to enhance their military power. For example, in response to Chinese strategic interest in AI, DIUx proposed greater scrutiny and restrictions on Chinese investment in Silicon Valley companies (Simonite, 2017). This behavior typifies a broader concern that synergies created by China’s civil-military fusion strategy could allow the technology, expertise, and intellectual property shared between US and Chinese commercial entities to be transferred to the PLA (Bartholomew and Shea, 2017 p. 507).

Moreover, broader national security concerns relating to Chinese efforts to catch up (and even surpass) the US in several critical security technologies, has prompted Washington to take increasingly wide-ranging and draconian steps (e.g., tightened US restrictions targeting China’s Huawei and its fledgling computer chip manufacturers) to counter this *perceived* national security threat. Against the backdrop of deteriorating US–China relations, responses such as these could accelerate the decoupling of cooperative bilateral ties between these two poles; increasing the likelihood of strategic competition, mutual mistrust, and negative action–reaction dynamics known as a security dilemma – which continue to manifest in other military technologies, including missile defense, hypersonic weapons, and counter-space capabilities (Jervis, 1976, chapter 3; Johnson, 2017 pp. 271–288).

Washington’s alarmist tone and policy responses to the perceived threat posed by China’s emerging security technology reveals that when we compare the public narratives surrounding the ‘new multipolarity’ thesis with what is happening two things emerge (Zala, 2017 pp. 2–17).

First, the nature of great power competition in emerging security technologies suggests that a shift to Sino–US bipolarity (and not multipolarity) is more likely in the short-to-medium term. Second, even if China surpasses the US in emerging security technologies, China still trails the US in several qualitative measures that coalesce to preserve its technological leadership (Lee, 2018). The United States has the world’s largest intelligence and R&D budgets, world-leading technology brands, academic research and innovation (discussed later in the chapter), and the most advanced (offense and defensive) cyber capabilities. Whether these advantages will be enough for Washington to forestall a shift in the military balance of power in the event China catches up or leap-frogs the US in AI – either through mimicry, espionage, or indigenous innovation – and can convert these gains (at a lower cost and less effort than the US) into potentially game-changing national security capabilities is, however, an open question.

China is by some margin Washington’s closest peer-competitor in emerging security technology. Beijing’s 2017 ‘Next Generation AI Development Plan’ identified artificial intelligence as a core “strategic technology” and a new focus of “international competition.” China’s official goal is to “seize the strategic initiative” (especially vis-à-vis the US) and achieve “world-leading levels” of investment in emerging security technologically such as AI by 2030 – targeting more than US\$150 billion in government investment (The State Council Information Office, 2017). Further, Beijing has leveraged lower barriers of entry to collect, process, and disseminate data within China to assemble a vast database to train AI systems. According to a recent industry report, China is on track to possess 20 percent of the world’s share of data by 2020, and the potential to have over 30 percent by 2030 (Knight, 2017).

State-directed Chinese investment in the US AI market has also become increasingly active and, in several instances, Chinese investment has competed in direct competition with the DoD (Kania, 2017). In 2017, for example, a Chinese state-run company Haiyin Capital outmaneuvered the US Air Force’s efforts to acquire AI software developed by Neurala in 2017 (Mozur and Perlez, 2017). Incidences such as these are indicative of broader US concerns related to China’s willingness (or propensity) to resort to industrial espionage and other means (i.e., forcing foreign-partners of China-based joint ventures to divulge their technology), to gain access to US AI technology, in an effort to catch up with, and leap-frog, the US in a range of strategically critical dual-use technologies (e.g., semiconductors, robotics, 5G networks, cyberspace, the internet of things, big data analytics, and quantum communications) (Lo, 2019). Industrial espionage can, however, only take the Chinese so far. The development of China’s national innovation base, expertise, and capacity – even if that foundation builds on industrial and other types of espionage and mimicry – is a broader trend of which the DoD also appears to be cognizant (US Department of Defense, 2019b p. 96).

Among these critical enabling technologies that could fundamentally change modern warfare are next-generation data transmission networks. The strategic importance of 5G networks as a critical military technological enabler was demonstrated during the protracted tensions between China’s Huawei and Washington. Experts view 5G as a cornerstone technology to increase the speed, stability data-loads, reduce the latency (i.e., accelerate network response times), and enhance mobile digital communications. According to an AI and telecommunications researcher at the University of Electronic Science and Technology of China, “the 5G network and the internet of things (IoT) enlarge and deepen the cognition of situations in the battlefield by several orders of magnitude and *produce gigantic amounts of data, requiring AI to analyze and even issue commands*” (Zhen, 2019, emphasis added).

In sum, against the backdrop of rising tensions in the US–China relationship on a plethora of interconnected policy arenas – for example, trade and geopolitical influence in the Indo-Pacific – the technological race for access and control of critical enablers that will connect

sensors, robotics, autonomous weapons systems, and the exchange of vast volumes of data in real-time through AI-machine learning techniques on the digitized battlefield, will become increasingly intense and strategically motivated (Kania and Costello, 2018 p.5).

### **China's Response to *Pax Americana* in Emerging Security Technology**

In 2017, Chinese President Xi Jinping explicitly called for the acceleration of the military 'intelligentization' agenda, to better prepare China for the development of modern warfare against a near-peer adversary, namely the United States (Xinhua, 2017). Although nascent Chinese think-tanks and the academic discourse are generally poor at disseminating their debates and content, open-source evidence suggests a strong link between China's political agenda related to the 'digital revolution,' Chinese sovereignty and national security, and the current public debate surrounding the rejuvenation of the Chinese nation as a great power. In short, national security is ultimately interpreted by China (and the United States) as encompassing economic performance.

President Xi's Belt-and-Road-Initiative (BRI), and the virtual dimension of the 'Digital Silk Road,' are high-level efforts designed to ensure that the mechanisms, coordination, and state-level support for this agenda will become increasingly normalized (Yuan, 2017). Xi recently stated that emerging security technologies, including AI, 'big data,' cloud storage, cyberspace, and quantum communications, were amongst the "liveliest and most promising areas for civil-military fusion." Towards this end, Xi has pledged additional state support and resources to enhance China's economic and military dimensions of its national power (Li, 2015; Lee and Sheehan, 2018). While BRI investment is predominantly in emerging markets with comparably low levels of technology maturity, human capital, and military power, the BRI framework supports a broader Chinese agenda to expand (or establish a new) geopolitical sphere of influence; to improve its position in the distribution of power – especially vis-à-vis the United States.

In the case of quantum technology, the potential convergence between AI and quantum computing could create promising synergies that Beijing intends to leverage to ensure it is at the forefront of the so-called 'quantum AI revolution.' Chinese analysts and strategists anticipate that quantum technologies will radically transform modern warfare, with a strategic significance equal to nuclear weapons. In 2015, for example, Chinese researchers reportedly achieved a breakthrough in the development of quantum machine learning algorithms, which could relieve several military-technological bottlenecks (e.g., quantum radar, sensing, imaging, metrology, and navigation). This allowed for greater Chinese independence from space-based systems – where it currently lags the US – enhance intelligence, surveillance, and reconnaissance capabilities; potentially creating new vulnerabilities in US space-based GPS and stealth technology in conflict scenarios in the Indo-Pacific (Kania and Costello, 2018 p. 18).

The evidence suggests a strong link between Beijing's pursuit of leadership in emerging security technologies and its broader geopolitical objectives in the Indo-Pacific. This link has, in turn, reinforced the narrative within Washington that China believes this technological transformation is an opportunity to strengthen its claim on the leadership – and eventual dominance – of the emerging technological revolution, having missed out on previous waves (Godement, 2018 pp. 1–5). In short, despite the clear economic issues at stake (i.e., the rents to be captured in the data-driven economy), the threat to US technological leadership is generally interpreted through military and broader geopolitical lens.

In contrast, the increasingly strained relationship between the Trump administration and Silicon Valley will likely pose additional challenges to this critical partnership in the development

of emerging security technologies for the US military. Following a high-profile backlash from employees at Google, for example, the company recently announced that it would discontinue its work with the Pentagon on Project Maven – a Pentagon program to build an AI-powered surveillance platform for unmanned aerial vehicles (White, 2018). Several defense analysts and US government reports have noted the growing gap between the rhetoric and the research momentum (especially in AI and robotics), and the paucity of resources available, to make the US military more networked and integrated (Harris, 2018).

Taken together, these reports highlight various shortcomings in the US defense innovation ecosystem such as inadequate funding to sustain long-term research and development (R&D), institutional stove piping inhibiting multi-disciplinary collaboration, and an insufficient talent pool to attract and retain top scientists in emerging security technological related fields (US Department of Defense, 2017). In its debut AI strategy, *Artificial Intelligence Strategy*, for example, the DoD committed to “consult with leaders from across academia, private industry, and the international community” and “invest in the research and development of AI systems” (US Department of Defense, 2019 p. 5). Details of the implementation and funding arrangements for these broad principles remain mostly absent, however. Moreover, the apparent mismatch (even dissonance) between the rapid pace of commercial innovation in emerging security technologies and the lagging timescales and assumptions that underpin the US DoD’s existing procurement processes and practices may exacerbate these bilateral competitive pressures (Kennedy and Lim, 2016 pp. 553–572).

China’s pursuit of AI-related (especially dual-use) technologies will fuel the perception (accurate or otherwise) in Washington that Beijing is *intent* on exploiting this strategically critical technology to fulfill its broader revisionist goals in the Indo-Pacific. That is, once the ‘digital silk road’ initiative reaches fruition, the BRI could enable China’s 5G, artificial intelligence and precision navigation systems to monitor and dominate the IoT, digital communications and intelligence of every nation within the BRI sphere of influence, as part of Beijing’s strategic objective, to ensure the leadership of a new Indo-Pacific, and eventually international, order. That is, China’s version of the Greater East Asia Co-Prosperty sphere, or Halford Mackinder and Mahan’s theories of world control and power distribution (Beasley, 1991).

In addition to this unique scaling advantage, Chinese national security innovation has also benefited from its approach to security technology acquisition: A centralized management system where few barriers exist between commercial, academic, and national security decision making. While most external analysts consider China’s centralized approach to the development of emerging security technology grants it unique advantages over the US, others posit that Beijing’s innovation strategy is far from perfect. Some analysts, for example, have characterized China’s state-directed funding arrangements as highly inefficient. Analysts note that China’s state apparatus is inherently corrupt and that this approach tends to encourage overinvestment in particular projects favored by Beijing, which may exceed market demand (He, 2017). For instance, though China has already surpassed the US in the quantity of AI-related academic research papers produced between 2017 and 2018, the quality of these papers ranks far below US academic institutions (Castro et al., 2019).

Besides, China is currently experiencing a shortage of experienced engineers and world-class researchers to develop AI algorithms. For instance, China has only thirty universities that produce indigenous experts and research products. As a result, industry experts have cautioned that Beijing’s aggressive and centralized pursuit of emerging security technologies such as AI, could result in poorly conceptualized capabilities that adversely impact the reliability and safety of advanced technologically augmented weapon systems (Barton and Woetzel, 2017).

The comparatively measured pace of US emerging security technological innovation might, therefore, in the longer run result in more capable tools, but without sacrificing safety for speed – even at the cost of falling behind China’s AI quantitative lead in the short term. The prioritization by the US of the development of robust, verifiable, and safe military AI technology might, however, come under intense pressure if China’s progress in dual-use AI is perceived as an imminent threat to the US first-mover advantages.

### **Arms Racing Dynamics in Emerging Security Technology in the Indo-Pacific**

As the most powerful nation-states in the Indo-Pacific and globally, leaders in the development of AI, the competitive tensions between China and the US have often evoked comparisons with the Cold War-era US–Soviet space race. In response to the global AI arms race, and to sustain US superiority and first-mover advantages in AI, US General John Allen and Spark Cognition CEO Amir Husain have argued that the US must push further and faster to avoid losing the lead to China (and to a lesser degree Russia) in the development of AI (Allen and Husain, 2017).

While these depictions accurately reflect the *nature* of the increasingly intense competition in the development of security technologies, the *character* of this emergent arms race intimates a much more multipolar reality. Over time, this trend will likely elevate technically advanced small and middle-powers (e.g., South Korea, Singapore, New Zealand, and Australia) to become pioneers in cutting-edge dual-use AI-related technology, and key influencers shaping the security, economics, and global norms, and standards of these innovations in the international political order.

In the Indo-Pacific, several states have already begun to develop emerging security technologies that will likely have second- and third-order effects as these technologies mature and are integrated into national security structures (Saalman, 2019 pp. 33–39). South Korea, for example, has developed a semi-autonomous weapon system to protect the demilitarized zone from North Korean aggression (the SGR-A1). Today, however, South Korea continues to lag behind other countries in the development of AI technology, in large part, due to the lack of AI-related investment and R&D. Singapore’s ‘AI Singapore’ initiative is a commercially driven US\$110 million effort to support AI R&D (Barsade and Horowitz, 2018). Although this level of government funding is relatively modest compared to other states (notably China), Singapore plans to use its business-friendly investment climate and established research clusters to attract companies to advance Singapore’s broader national R&D efforts in emerging technology.

While this broader trend will not necessarily run in lockstep with the US–China bipolar contest, it will inevitably be influenced and shaped by the ongoing competition between China and the United States (and its allies in the Indo-Pacific) on setting global technological standards for AI, nonetheless. For these middle-powers, the outcome of this contest, and in particular, how they position themselves on AI technology standards, will have a significant impact on their ability to truly become cutting-edge innovators in emerging security technology like AI – and independent of China and the United States. The commercial driving forces underlying emerging security technologies (i.e., hardware, software, and R&D), together with the inherently dual-use nature of these innovations, reduce the usefulness of the space race analogy (Organski and Kugler, 1980; Gilpin, 1981). In short, the particular problem-set associated with the Cold War-era bipolar structure of power is, to date, at least, far less intense in the context of contemporary competition in emerging security technologies (Gilli and Gilli, 2019 pp. 141–189).



The growing sense, the proliferation of AI technologies driven by powerful commercial forces will inevitably accompany (and even accelerate) the shift toward multipolarity. Above all, the risks associated with the proliferation and diffusion of dual-use security technologies across multiple sectors and expanding knowledge bases is a very different prospect compared to arms-racing between great power military rivals. Thus, the development of emerging security technologies based on military-centric R&D would make it much more difficult and costly for smaller (and especially less technically advanced) states to successfully emulate and assimilate (Brooks, 2006).

Moreover, military organization, norms, and strategic cultural interests and traditions will also affect how security technology is assimilated by militaries, potentially altering the balance of military power (Johnstone, 1995 pp. 65–93). As a result, the interplay of technology and military power will continue to be a complex outcome of human cognition, institutions, strategic cultures, judgment, and politics (Biddle, 2006). Ultimately, success in sustaining or capturing the first-mover advantages in AI will be determined by how militaries develop doctrine and strategy to seize on the potential comparative benefits afforded by AI-augmented capabilities on the battlefield (Johnson, 2020a).

The pace of military-use security technologies like AI to smaller-medium powers in the Indo-Pacific (e.g., Singapore, South Korea, Taiwan, Australia, and New Zealand) will also be constrained by three core features of this emerging phenomenon: (1) Hardware constraints (e.g., physical processors), and integrating increasingly sophisticated software and hardware with internal correctness; (2) the algorithmic complexity inherent to AI machine learning approaches; and (3) the resources and know-how to effectively deploy algorithmic code for AI machine learning (Ayoub and Payne, 2016 p. 809). The advantages China derives from its commercial lead in the adoption of emerging security technologies and dataset ecosystem will not necessarily be easily directly translated into special-purpose military applications (Castro et al., 2019).

China's strengths in commercial-use security technologies, including 5G networks, e-commerce, e-finance, facial recognition, and various consumer and mobile payment applications, will, therefore, need to be combined with specialized R&D and dedicated hardware – to unlock their potential dual-use military applications and augment advanced weapon systems. Absent requisite resources, know-how, datasets, and technological infrastructure, these constraints could make it very difficult for a new entrant to develop and deploy modular AI with the same speed, power, and force as China or the United States (Gray, 2015 pp. 1–6).

For instance, China and the United States are in close competition to develop the supercomputers needed to collect, process and disseminate the vast amounts of data that traditional computers can handle. While the United States possesses more powerful computers, China trumps the US in terms of the number of supercomputers. Thus, military-led innovations could potentially concentrate and consolidate leadership in this nascent field amongst current military superpowers (i.e., China, the US, and to a lesser extent Russia), and revive the prospect of bipolar competition (Bostrom, 2014). For now, it is unclear how specific emerging security technologies may influence military power, or whether, and in what form these innovations will translate into operational concepts and doctrine (Cummings, 2017).

In sum, the degree to which AI alters the military balance of power will depend in large part on the speed of the diffusion of this technology within the military structures of the United States, China, and other states in Indo-Pacific such as Singapore, South Korea, and Japan. As the tectonic plates of the global political system continue to shift, the United States and China are on opposite sides of the divide, and China's neighbors – in particular US allies and partners in the region – will need to pick a side and choose whether to work with or separately from

the United States – its credibility, legitimacy and ability to impose its will are fast eroding – or side with China. Against the backdrop of geopolitical tensions and mounting apprehension about the future of US policy in the Indo-Pacific, the function of human innovation, political agendas, and strategic calculation and judgment, and heuristic decision making (or the propensity for compensatory cognitive short-cuts) associated with decisions taken under compressed timeframes in uncertain and complex environments will become increasingly important for how emerging security technologies develop in the region.

## **Conclusion**

The chapter's key takeaways can be summarized as follows. First, while disagreement exists on the likely pace, trajectory, and scope of security technological innovations, a consensus is building within the US defense community intimating that the potential impact of security technologies such as AI on the distribution of power and the military balance will likely be transformational, if not revolutionary. These assessments have, in large part, been framed in the context of the perceived challenges posed by revisionist and dissatisfied great military powers (i.e., China and Russia) to the current US-led international order – i.e., its rules, norms, and governing structures.

Second, the rapid proliferation of high-tech defense innovations exists concomitant with a growing sense that the United States has dropped the ball in the development of these disruptive security technologies. Even the perception that Washington's first-mover advantage in a range of dual-use enabling critical security technologies (i.e., semiconductors, 5G networks, and IoT's) was at risk from rising – especially nuclear-armed – military powers such as China, the implications for security and stability in the Indo-Pacific could be severe. In response to a growing sense of urgency within the US defense community cognizant of this prospect, the Pentagon has authored several AI-related programs and initiatives designed to protect US dominance on the modern digitized battlefield.

Third, and related to the previous finding, in the development of security technologies, evocations of the Cold War-era space race do not accurately capture the nature of this rapid and expansive disruptive technological phenomena. Instead, compared to the bipolar features of the US-Soviet struggle, this innovation arms race intimates more multipolar characteristics. Above all, the dual-use and commercial drivers of the advances in emerging security technology will likely narrow the innovation gap separating great powers in the Indo-Pacific – chiefly the US and China – and other technically advanced small-medium powers in the region. In the longer term, these emerging powers will become critical influencers in shaping security, economics, and global norms in dual-use security technology.

In the case of military-centric technologies, however, several coalescing features of this trend – hardware constraints, machine-learning algorithmic complexity, and the resources and know-how to deploy military-centric AI code – will likely in the near-term constrain the fusion of these security technologies with weapon systems. In turn, these constraints could further concentrate and consolidate the leadership in the development of these critical technological enablers amongst the current military great powers (i.e., China, the United States, and to a lesser degree Russia), causing resurgent bi-polar strategic competition. As China approaches parity (and possibly surpasses) the US in several emerging security technologies fields like AI, therefore, it will increasingly view any technological progress by China through a national security lens, and broader US-China geopolitical tensions in the Indo-Pacific and globally (Waltz, 1979).

## Note

- 1 Recent progress in AI falls within two distinct fields: (1) 'narrow' AI, and particularly, machine learning; (2) 'general' AI, which refers to AI with the scale and fluidity akin to the human brain.

## References

- Acton, J. M. (2013). *Silver Bullet? Asking the Right Questions about Conventional Prompt Global Strike*. Washington, DC: Carnegie Endowment for International Peace.
- Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security*. Cambridge, MA: Belfer Centre for Science and International Affairs.
- Allen, J. R., & Husain, A. (November 3, 2017). 'The Next Space Race is Artificial Intelligence. *Foreign Policy*. <https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/>, accessed November 10, 2018.
- Ayoub, K., & Payne, K. (2016). Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies*, 39(5–6), 793–819. doi:10.1080/01402390.2015.1088838
- Bartholomew, C., & Shea, D. (2017). *US-China Economic and Security Review Commission – 2017 Annual Report*. Washington, DC: The US-China Economic and Security Review Commission.
- Barton, D., and Woetzel, J. (2017). *Artificial Intelligence: Implications for China*. New York, NY: McKinsey Global Institute.
- Beasley, W. G. (1991). *Japanese Imperialism 1894–1945*. Oxford, UK: Clarendon Press.
- Beverchen, A. (2007). Clausewitz and the Non-Linear Nature of War: Systems of Organized complexity. In H. Strachan & A. Herberg-Rothe (Eds.), *Clausewitz in the Twenty-First Century* (pp. 45–56). Oxford: Oxford University Press.
- Barsade, I., and Horowitz, M. C. (August 16, 2018). 'Artificial intelligence beyond the superpowers,' *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/>, accessed August 20, 2019.
- Biddle, S. (2006). *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton, NJ: Princeton University Press.
- Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.
- Boulanin, V. (Ed.). (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk Vol. I Euro-Atlantic Perspectives*. Stockholm: SIPRI Publications.
- Brooks, S. G. (2006). *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict*. Princeton, NJ: Princeton University Press.
- Castro, D., McLaughlin, M., & Chivot, E. (2019). *Who is Winning the AI Race: China, the EU, or the United States?* Washington, D.C.: Center for Data Innovation.
- Cummings, M. L. (2017). *Artificial Intelligence and the Future of Warfare*. London, UK: Chatham House.
- Geist, A. E., & Lohn, J. (2018). *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Santa Monica, CA: RAND Corporation.
- Gilli, A., & Gilli, M. (2019). Why China has not Caught up Yet. *International Security*, 43(3), 141–189. doi:10.1162/isec\_a\_00337
- Gilpin, R. (1975). *US Power and the Multinational Corporation: The Political Economy of Foreign Direct Investment*. New York, NY: Basic Books.
- Godement, F. (2018). *The China Dream Goes Digital: Technology in the Age of Xi*. Paris: European Council on Foreign Affairs ECFC, pp. 1–5.
- Gray, E. (2015). Small Big Data: Using Multiple Datasets to Explore Unfolding Social and Economic Change. *Big Data & Society*, 2(1), 1–6. doi:10.1177/2053951715589418
- Hadley, D. & Nathan, L. (2017). *Artificial Intelligence and National Security*. Congressional Research Service, Washington, DC.
- Harris, A. H. B. Jr., (2018, March 2). *The Integrated Joint Force: A Lethal Solution for Ensuring Military Preeminence*. Strategy Bridge. <https://thestrategybridge.org/the-bridge/2018/3/2/the-integrated-joint-force-a-lethal-solution-for-ensuring-military-preeminence> accessed May 4, 2019.
- He, Y. (2017). *How China is Preparing for an AI-powered Future*. Washington, DC: The Wilson Center.
- Horowitz, M. C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. *Texas National Security Review*, 1(3), 37–57.
- Jervis, R. (1976). *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press.

- Johnson, J. (2017). Washington's Perceptions and Misperceptions of Beijing's Anti-Access Area-Denial (A2-AD) 'Strategy': Implications for Military Escalation Control and Strategic Stability. *The Pacific Review*, 30(3), 271–288. doi:10.1080/09512748.2016.1239129
- Johnson, J. (2019a). Artificial Intelligence & Future Warfare: Implications for International Security. *Defense & Security Analysis*, 35(2), 147–169. doi:10.1080/14751798.2019.1600800
- Johnson, J. (2019b). The AI-cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability. *Journal of Cyber Policy*, 4(3), 442–460. doi: 10.1080/23738871.2019.1701693
- Johnson, J. (2019c). The End of Military-techno Pax Americana? Washington's Strategic Responses to Chinese AI-enabled Military Technology. *The Pacific Review*. doi: 10.1080/09512748.2019.1676299
- Johnson, J. (2020a). Artificial Intelligence: A Threat to Strategic Stability. *Strategic Studies Quarterly*, 14(1), 16–39. doi:10.2307/26891882
- Johnson, J. (2020b). Delegating Strategic Decision-Making to Machines: Dr. Strangelove Redux? *Journal of Strategic Studies*. doi: 10.1080/01402390.2020.1759038
- Johnson, J. (2020c). Artificial Intelligence in Nuclear Warfare: A Perfect Storm of Instability? *The Washington Quarterly*, 43(2), 197–211. doi: 10.1080/0163660X.2020.1770968
- Johnson, J. (2021). *Artificial Intelligence & the Future of Warfare: USA, China, and Strategic Stability*. Manchester, UK: Manchester University Press.
- Johnston, A. I. (1995). Thinking about Strategy Culture. *International Security*, 19(4), 32–64. doi:10.2307/2539119
- Kania, E. (2017). *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Washington, DC: Centre for a New American Security.
- Kania, E. B., & Costello, J. K. (2018). *Quantum Hegemony? China's Ambitions and the Challenge to US Innovation Leadership*. Washington, D.C.: Center for a New American Security.
- Kennedy, A. (2016). Slouching Tiger, Roaring Dagon: Comparing India and China as Late Innovators. *Review of International Political Economy*, 23(1), 65–28. doi:10.1080/09692290.2015.1105845
- Kennedy, A., & Lim, D. (2017) The Innovation Imperative: Technology and US-China Rivalry in the Twenty-first Century. *International Affairs*, 94(3), 553–572.
- Knight, W. (October 10, 2017). China's AI Awakening. *MIT Technology Review*. www.technologyreview.com/2017/10/10/148284/chinas-ai-awakening/, accessed October 1, 2019.
- Layne, C. (2012). This Time it's Real: The End of Unipolarity and the Pax Americana. *International Studies Quarterly*, 56(1), 203–213. doi:10.1111/j.1468-2478.2011.00704.x
- Lee, K.-F., & Sheehan, M. (2018). China's Rise in Artificial Intelligence: Ingredients and Economic Implications. Hoover Institution. www.hoover.org/research/chinas-rise-artificial-intelligence-ingredients-and-economic-implications, accessed April 5, 2019.
- Li, R. (March 3, 2015). China Brain' Project Seeks Military Funding as Baidu Makes Artificial Intelligence Plans. *South China Morning Post*. www.scmp.com/lifestyle/article/1728422/china-brain-project-seeks-military-funding-baidu-makes-artificial, accessed February 1, 2018.
- Lo, K. (January 16, 2019). China says US Claims it Uses Forced Technology Transfer to Boost Military are 'Absurd.' *South China Morning Post*. www.scmp.com/news/china/military/article/2182402/china-says-us-claims-it-uses-forced-technology-transfer-boost, accessed October 5, 2019.
- Moore, A. W. (November 1, 2017). *AI and National Security in 2017*. Presentation at AI and Global Security Summit, Washington, DC.
- Mozur, P., & Perlez, J. (March 22, 2017). China Bets on Sensitive US Start-ups, Worrying the Pentagon. *The New York Times*. www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html, accessed October 11, 2019.
- Opinions on Strengthening the Construction of a New Type of Think Tank with Chinese Characteristics. (October 27, 2015). *China Daily*. www.chinadaily.com.cn/china/2014-10/27/content\_18810882.htm, accessed April 1, 2017.
- Organski, A. F. K., & Kugler, J. (1980). *The War Ledger*. Chicago: University of Chicago Press.
- Roff, H. M. (2019). The Frame Problem: The AI "Arms Race" Isn't One. *Bulletin of the Atomic Scientists*, 75(3), 1–5.
- Saalman, L. (Ed.). (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk Vol. II East Asian Perspectives*. Stockholm: SIPRI Publications.
- Schelling, T. C., & Halperin, M. H. (1975). *Strategy and Arms Control*. Washington, DC: Pergamon-Brassey.
- Simonite, T. (2017, November 8). Defense Secretary James Mattis Envis Silicon Valley's AI ascent. *Wired.com*. www.wired.com/story/james-mattis-artificial-intelligence-diux/, accessed April 1, 2018.

- The State Council Information Office of the People's Republic of China. (2017, July 20). State Council Notice on the Issuance of the New Generation AI Development Plan.
- US Department of Defense (2019b). *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2019*. Washington, DC: US Department of Defense.
- US Department of Defense (2017). *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2017*. Washington, DC: US Department of Defense.
- US Department of Defense (2016, February 2). *Remarks by Secretary Carter on the Budget at the Economic Club of Washington*.
- US Department of Defense (2019a). *Lt. Gen. Jack Shanahan Media Briefing on A.I.-related Initiatives within the Department of Defense*. Washington, DC: US Department of Defense.
- US Department of Defense, Lt. Gen. Jack Shanahan Media Briefing on AI-Related Initiatives within the Department of Defense, (August 20, 2019). [www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/Lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/](http://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/Lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/), accessed April 21, 2019.
- Waltz, K. (1979) *Theory of International Politics*. Reading, MA: Addison-Wesley.
- White, J. (June 7, 2018) Google Pledges not to Work on Weapons after Project Maven Backlash. *The Independent*. [www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-weapons-military-project-maven-sundar-pichai-blog-post-a8388731.html](http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-weapons-military-project-maven-sundar-pichai-blog-post-a8388731.html), accessed January 1, 2019.
- White House. (2019). Executive Order on Maintaining American Leadership in Artificial Intelligence. (2019, February 11). [www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/](http://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/), accessed January 1, 2018.
- Wilkening, D. (2019). Hypersonic Weapons and Strategic Stability. *Survival*, 61(5), 129–148. doi:10.1080/00396338.2019.1662125
- Work, R. O. (2015, July). *Remarks by Defense Deputy Secretary Robert Work at the CNAS Inaugural National Security Forum, Speech, CNAS Inaugural National Security Forum*. Washington, DC: CNAS.
- Work, R. O., & Brimley, S. W. (2014). *20YY Preparing for War in the Robotic Age*. Washington DC: Center for a New American Security.
- Xi Jinping's Report at the 19th Chinese Communist Party National Congress. (October 27, 2017). *Xinhua*. [www.xinhuanet.com/english/special/2017-11/03/c\\_136725942.htm](http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm) accessed January 1, 2020).
- Yuan, W. (November 3, 2017). China's 'Digital Silk Road': Pitfalls Among High Hopes. *The Diplomat*. <https://thediplomat.com/201711/chinas-digital-silk-road-pitfalls-among-high-hopes/>, accessed January 1, 2018.
- Zala, B. (2017). Polarity Analysis and Collective Perceptions of Power: The Need for a New Approach. *Journal of Global Security Studies*, 2(1), 2–17. doi:10.1093/jogss/ogw025
- Zhen, L. (January 31, 2019). Why 5G, a Battleground for US and China, is Also a Fight for Military Supremacy. *South China Morning Post*. [www.scmp.com/news/china/military/article/2184493/why-5g-battleground-us-and-china-also-fight-military-supremacy](http://www.scmp.com/news/china/military/article/2184493/why-5g-battleground-us-and-china-also-fight-military-supremacy), accessed October 10, 2019.