NIDS International Symposium on Security Affairs 2021

Technological Innovation and Security: The Impact on the Strategic Environment in East Asia

The National Institute for Defense Studies, Japan

NIDS International Symposium on Security Affairs 2021

Technological Innovation and Security: The Impact on the Strategic Environment in East Asia

The National Institute for Defense Studies

NIDS International Symposium on Security Affairs 2021

Technological Innovation and Security: The Impact on the Strategic Environment in East Asia

Date of publication: September 2022
Editor, publisher: The National Institute for Defense Studies

5-1 Ichigaya Honmuracho, Shinjuku-ku, Tokyo 162-8808, Japan
www.nids.mod.go.jp/english

This publication is a collection of papers originally presented at the 22nd *International Symposium on Security Affairs*, hosted online by the National Institute for Defense Studies (NIDS) on December 8, 2022 from Tokyo. The views and opinions of the authors expressed in this publication are personal and do not necessarily state or reflect those of the respective organizations to which they belong, nor of any national government.

NIDS is a research and educational institution of the Ministry of Defense, carrying out academic and policy-oriented research into issues of defense, security and military history, as well as the education of Japan Self-Defense Forces officers and civilian officials of the Ministry. NIDS also organizes exchanges with defense research institutions overseas, particularly national defense universities.

ISBN 978-4-86482-111-7
Translated and printed by INTERBOOKS

Contents

Chairperson's Summary

The National Institute for Defense Studies (NIDS) held the International Symposium on Security Affairs in virtual format on December 8, 2021. The theme was "Technological Innovation and Security: The Impact on the Strategic Environment in East Asia." This symposium was intended not only to foster security dialogue but also to improve research quality, stimulate interaction, promote mutual understanding among the international public and experts, and contribute to security policy.

The symposium was divided into two parts. Session 1 examined technological innovation and security from the perspectives of the United States (U.S.), Japan, and China and Session 2 from the perspectives of Australia, Singapore, and Russia. In addition, a keynote speech was delivered between the two sessions. Each session consisted of presentations by panelists followed by discussion and Q&As with panelists.

Below is a summary of the symposium's Session 1, keynote speech, and Session 2, in that order. In Session 1, presentations were made from the "Perspectives of the U.S., Japan, and, China" by Mr. Bryan Clark (Senior Fellow & Director, Center for Defense Concepts and Technology, Hudson Institute), Dr. Fujita Motonobu (Policy Coordinator; Technology Policy Office; Technology Strategy Division; Department of Technology Strategy; Acquisition, Technology and Logistics Agency [ATLA]), and Dr. Tai Ming Cheung (Director, Institute on Global Conflict and Cooperation [IGCC], University of California). Mr. Iida Masafumi (Head; America, Europe, and Russia Division; NIDS) conducted the discussion with the panelists.

The first speaker, Mr. Clark, gave a presentation titled "Technological Innovation and Security: A U.S. Perspective." He discussed the transition from the "era of craftsmen," in which a small number of soldiers used handmade weapons, to the "era of homogeneity and scale" characterized by the Industrial Revolution and mechanization, and now to the "era of heterogeneity at scale." He described that civilian technological innovation is bringing an end to the industrial era as we know it, a period in which weapons manufacturing ability has been the deciding factor in victory or defeat.

He noted that the Chinese People's Liberation Army (PLA) is pursuing modernization, and industry-driven innovation has reached its pinnacle. He further noted that China has the capacity to produce weapons in large quantities, and that the scale of the PLA now surpasses that of U.S. allies.

He noted that, meanwhile, the U.S. military is attempting to incorporate artificial

intelligence (AI) and autonomous systems. Called decision-centric warfare or Mosaic Warfare, this approach is characterized by decision-making in the field, which creates more options and therefore widens the scope of decisions while delaying the enemy's decision making. He pointed out that forces are being distributed based on these concepts, and that distribution is increasing the options available to commanders. Integrating unmanned platforms with manned platforms is an example of this warfare. Other examples include the space domain, where the U.S. military is shifting from a small number of large satellites to constellations of low earth orbit satellites. In addition, he said the U.S. military is attempting to leverage human command and machine control to make full use of its distributed forces. The combination of human command and machine control, in which machines propose options, is already in practical use in the Air Force's refueling. AI is also assisting in decision making. He noted the U.S. military is working to increase options leading to escalation, stating that distributed forces would enable moving up and down the escalation ladder, and that conversely, adversaries would be unable to respond unless various countermeasures are taken.

The second speaker, Dr. Fujita, offered a Japanese perspective in his presentation entitled, "Potential Impact of Advanced Technologies on Future Contested in Asia-Pacific." He explained that the significance of state investments in technology lies in its use as a means of inter-state competition, and that concentrated investment in a particular technology was a statement of national intent. While there is no stable definition of emerging technologies, for the purposes of his presentation, he referred to technologies that have a broad impact on doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) as emerging technologies.

He pointed out that Japan's Ministry of Defense (MOD) has released two strategic documents regarding technology. One is the Strategy on Defense Production and Technological Bases, formulated in 2014, which he said is characterized by its provision for agile selection of acquisition methods. The other document is the Defense Technology Strategy, formulated in 2016, which he said is distinct for its presentation of investment portfolios. Group 1 portfolios represent fields in which Japan always has superiority over other countries, such as advanced material technologies, and in which MOD will actively invest resources. Group 2 corresponds to fields in which Japan will be at a strategic disadvantage without a certain technological footing, and in which MOD will invest a certain amount of resources. The investment of resources in this group will be important from the perspective of maintaining the supply chain as well. Group 3 represents fields where technology is being developed by the private sector on its own initiative, and in

which MOD will not actively invest but will keep abreast of the trends.

Dr. Fujita then pointed out that MOD's research and development (R&D) budget over the past 30 years has fluctuated significantly due to big projects. He said MOD is presented with a new challenge—whether to continue investing in the development of a specific platform, or to prioritize investments in acquiring and strengthening capabilities in new domains such as space, cyber, and electromagnetic, or to increase the budget to realize both.

Lastly, he discussed the potential impact of individual technology fields on the Asia-Pacific region. He said electromagnetic spectrum (EMS) technology, especially directed energy weapons, could increase our options in the gray zone, while EMS management poses a major challenge in the application of this technology. He noted that Intelligence, Surveillance and Reconnaissance (ISR) technologies, including space technology, are essential for decision making from the strategic to the tactical levels, and simultaneously, that deception and concealment technologies will likely make advances to counter such technologies. He expected that cyber technology measures to keep equipment operational will become critical, and that unmanned and manpower-saving technologies will complement or partially replace conventional manned platforms. In addition, he noted that hypersonic technology shortens the response time of the side being attacked. He described that digital technology will become key in quantitatively forecasting the impact of emerging technologies, that simulations of electromagnetic warfare will become possible on calculators, and that digital technology will serve as a bridge between R&D departments and users.

The last speaker, Dr. Cheung, gave a presentation titled, "The Rise of the Chinese Techno-Security State and its Strategic Implications," for a Chinese perspective. He highlighted Xi Jinping's remarks that the nation's development will be achieved through innovation and that technological development is the most critical area. Dr. Cheung noted that the Xi administration places focus on linking innovation and security. He refers to states that prioritize these aspects as "techno-security states," and explained that this term applies not only to China but also to the U.S.

He noted that the Xi administration is accelerating the building of a techno-security state. It has formulated and promoted the National Security Strategy, the Innovation-Driven Development Strategy, Xi's Thought on Military Strengthening in the New Era, the Military-Civil Fusion Development Strategy, and economic securitization, aimed at strengthening China's military in the new era which includes achieving defense modernization by 2035 and becoming a world-leading military power by 2050. He

stated that, while military-civil fusion is still in its early stages, China perceives it must secure its entire economy in response to wide-ranging confrontations with the U.S., with emphasis on protecting China's economy from external threats, especially from a technological perspective.

He identified five factors in comparing the U.S. and Chinese techno-security states. First is the perception of external threats. He noted that China has viewed the U.S. as a techno-security threat since the late 1990s, while the U.S. has taken longer to view China as a serious techno-security concern. Second is leadership and management coordination, which he said is top-down in China and bottom-up in the U.S. Third is governance regime, where China relies on penalties to ensure compliance with laws and regulations, whereas the U.S. leverages incentives and rewards to ensure compliance with laws and regulations by the private sector. Fourth is hybridization. He said China is in the early stages of military-civil fusion, while the U.S. is in the mature stage of public-private hybridization. Fifth is dependence vs. primacy. He noted that China aims to secure technological self-reliance but remains highly dependent on foreign technology and know-how, while the U.S. has secured self-reliance and is exporting technology to other countries.

His overall assessment of the early 2020s was that China is more strongly motivated and politically committed to building techno-security capabilities, and that the U.S. advantage is gradually eroding.

Session 1's discussion began with comments and questions from Mr. Iida regarding the three presentations. He asked Mr. Clark a question regarding innovation and operations, respectively. Noting that the U.S. is transitioning from a centralized to a decentralized model of innovation, while China is pursuing state-led military innovation under a military-civil fusion policy, Mr. Iida asked whether China's distinctive approach to innovation is effective and whether the decentralized approach of the U.S. has advantages over China's approach in military technology innovation. With regard to operations, he wondered whether the U.S. did not have ethical barriers to granting a certain degree of decision-making authority to AI, and asked about the current and future prospects for military use of AI in the U.S.

Mr. Iida had two questions for Dr. Fujita. His first question concerned the advantages and disadvantages of China's approach, noting that China determines which technologies to invest in based on predictions about the future way of war, while Japan makes investment decisions taking the current technology as the starting point. His second question asked which technologies Japan should invest in considering Japan's

strategic environment and technological potential.

Dr. Cheung was asked about China's approach to technological development. Mr. Iida questioned the sustainability of the system that allows for state-led mobilization, such as the top-down model and military-civil fusion, and asked whether China's approach is effective for generating true innovations that are not advances in existing technologies. Regarding Dr. Cheung's remark about the declining U.S. advantage relative to China, Mr. Iida asked whether China's policies offer any lessons for the U.S. to regain its advantage and what factors could slow down the pace of Chinese innovation.

Mr. Clark noted that both the U.S. and China are developing the same technologies, such as hypersonic weapons and AI, but that the U.S. is developing them under a decentralized model with operators taking the initiative. He said the U.S. model makes it easier to draw on the insights of operators compared to the Chinese approach, which develops technologies by working backwards from future warfare projections. He described the U.S. model as an operations-focused model and China's as a technology-focused model.

Dr. Fujita, in answer to the first question, explained that the approach of Japan's Defense Technology Strategy is based on self-analysis. He said that if the self-analysis is appropriate, then Japan can make maximum use of the strengths of its technological bases. A disadvantage of this approach is inefficient capacity building when the needs of operators do not match the strengths of the technological bases. In order to prevent such a situation, he stressed the importance of dialogue between operators and the R&D community. He stated that the Chinese approach leads to efficient investment if the intelligentized warfare concept is materialized; however, a disadvantage of this approach is that investment becomes inefficient if the battle concept turns out to be erroneous. In response to the second question, Dr. Fujita stated that given Japan's geographical environment and demographics, it is important to have maritime autonomous systems. He emphasized that the key to their successful development is promotion of open system architecture that enables the participation of various actors.

Dr. Cheung noted that China's approach has allowed it to catch up with the technologies of other countries in a few decades, namely, by absorbing foreign technologies into both the military and civilian sectors and making further advancements domestically. President Xi Jinping, meanwhile, seeks to achieve innovation indigenously and has been reorganizing China's R&D structure, including the major research institutes. In addition, Dr. Cheung pointed out that China is focusing attention on a range of emerging technologies, motivated by the Xi regime's strong sense of urgency to

keep up with other countries, and that China is investing resources to lead technological innovation. Regarding what the U.S. can learn from China, he mentioned state-market balance. He explained that China has a state-led model as opposed to the market-led model of the U.S., and that the U.S. has an appropriate balance without excessive state intervention in the market.

From the audience, Dr. Fujita was asked whether costs and climate change are taken into account in defense equipment development. Mr. Clark was asked if the current air tasking cycle of the U.S. could be modified for the purposes of decentralized operations involving flexible and rapid decision making.

Dr. Fujita responded that cost is an important factor given the severe fiscal situation and that equipment development must be cost efficient. He stated that climate change had not been a major consideration, but that with the recent intensifying debate, the diversion of technology for climate change measures has been considered during the R&D process.

Mr. Clark mentioned that AI is already helping to speed up the air tasking cycle, noting that AI-assisted decision making can shorten a cycle of about 18 hours to a few hours. He also pointed out that AI's use is critical to enhancing human creativity through AI-assisted decision making. In fact, he said, a human can sometimes make a decision more quickly than AI because it presents too many choices and the computer does not have adequate resources. He thus pointed out that AI is not a replacement for humans but rather a tool to help humans become more creative.

For the keynote speech, Dr. Sunami Atsushi (President, Sasakawa Peace Foundation [SPF]; Executive Advisor to the President & Director, Science for RE-designing Science, Technology and Innovation Policy [SciREX] Center, National Graduate Institute for Policy Studies [GRIPS]) delivered an address titled, "Technological Innovation and Security: Japan's Innovation Strategy Based on Technological Patriotism." Dr. Sunami stated that a country must possess two systems to become a science and technology great power, and that these systems enabled the U.S. to establish techno-hegemony in the 20th century. They are: (1) a system of universities and for introducing their achievements to society through industry-academia collaboration; and (2) a system of mass production. He said that China today also possesses these two systems, and that the U.S. and China are engaged in a contest for supremacy as advanced technology giants.

In addition, Dr. Sunami made the point that advanced science and technology is important for expanding a country's sphere of activities into outer space, cyberspace, and other domains where humans have not yet expanded their sphere of activities, and that

possessing science and technology for this purpose will enable nations to occupy a key position in security. He noted that most advanced science and technology is dual-use: most advanced science and technology is dual-use technology, which transforms society and also has a critical role in security and a direct impact on military strategy. Against this backdrop, he explained that mission-type R&D, in which the state allocates resources to science and technology development based on societal issues and national interest needs, has become mainstream globally, and that nations are focusing investment especially in advanced technologies related to climate change and security and in technological infrastructure that support future industries. Furthermore, he noted that many of the special technologies that give rise to major changes do not fit the business models of private companies, that the government must strategically take the lead in developing emerging technologies which will be game changers, and that mission-type technology development has become the mainstream.

Dr. Sunami noted that the Biden administration is working to secure critical technologies by taking measures, such as the Executive Order on America's Supply Chains and the Innovation and Competition Act, and strengthening collaboration with allies. China, in contrast, through government-led resource allocation, is gradually establishing a national innovation system that produces advanced technologies without depending on foreign countries, aiming to become a world-leading manufacturing power by the 100th anniversary of China's founding in 2049. He expected Beijing to create a system similar to the U.S. innovation system, albeit China's largely government-led system differs in form and approach from the U.S. system which has the private domain at its core. He stated that Japan must also build a corresponding innovation system, and to this end, underscored the importance of industry-academia collaboration, including cooperating with universities on the development of dual-use technologies, and of establishing a system for the management of intellectual property and sensitive technology information. In order to develop advanced technologies with limited resources, he said that Japan needs to collaborate with other countries and establish a collaborative system for developing emerging and dual-use technologies with the U.S., Europe, and other partners. He concluded that frameworks such as bilateral cooperation, Five Eyes + Japan, and QUAD can serve as a platform for cooperation on the social implementation of advanced technologies, such as AI, quantum, and space technologies, and that this requires overcoming the challenges to cooperation, such as information and technology management and collaborative strategy formulation.

In Session 2, presentations were made from the "Perspectives of Australia, Singapore,

and Russia" by Dr. Malcolm Davis (Senior Analyst, Australian Strategic Policy Institute [ASPI]), Dr. Michael Raska (Assistant Professor, S. Rajaratnam School of International Studies [RSIS], Nanyang Technological University), and Dr. Ivan Danilin (Head, Department of Science and Innovation, Institute of World Economy and International Relations [IMEMO], Russian Academy of Sciences). Mr. Akimoto Shigeki (Senior Fellow, Policy Simulation Division, NIDS) conducted the discussion with the panelists.

Dr. Davis gave a presentation titled "Technological Change and Future Security in the Indo-Pacific: An Australian Perspective." Dr. Davis began by providing the strategic context of the current era of heightened uncertainty. He then discussed Australia's latest strategic documents, which recognize that the strategic competition between the U.S. and China will be the principal factor that defines the Indo-Pacific region, that high intensity military conflict between the two countries is becoming more likely, and that the traditional defense posture assumption of a ten-year warning time before a direct attack against Australia is no longer applicable. Regarding the strategic context, Dr. Davis emphasized the importance of AUKUS and QUAD as cooperative frameworks for the development and implementation of emerging military-related technologies. He noted that AUKUS, in particular, is a cooperative framework that goes beyond the sharing of submarine technology that is drawing attention, and that through cooperation on AI, quantum, cyber, hypersonic, space, and other technologies, AUKUS is expected to contribute to Australia's long-range strike capability and domestic manufacturing capacity. He expressed his hopes for QUAD in realizing cooperation on military-civil dual-use technologies, especially in the aforementioned areas. Furthermore, he expressed the view that Australia has entered an era which requires capabilities to project forces from the mainland to distant regions, such as Guam, the South China Sea, and the Taiwan Strait, in order to shape the regional situation, deter threats, and respond when deterrence fails.

Dr. Davis then discussed the impact of emerging technologies on future warfare. One of the specific issues he stressed was that the pace of development of emerging technologies and the pace of consideration of their future warfare uses at the concept level diverged from the actual pace of the equipment procurement cycle, pointing to the need to accelerate the procurement cycle. Dr. Davis noted that the future multi-domain operations environment will require human-machine teaming, predicting that the faster speed of operations and their increasing complexity will exceed the ability of human processing. In addition, he forecasted that China and Russia will have comparable capabilities, and noted the need to assume warfighting in circumstances where military

and technological advantages are undermined. As AI and autonomous systems take on a greater role, the nature of human involvement becomes a dilemma. Dr. Davis said it was necessary to consider the balance between delegation to autonomous systems and human intervention, as well as the risk of China, Russia, and other countries with different ethics than the West leading the introduction of autonomous systems. Concerning tangible trends, he mentioned transformation of space into a warfighting domain and the development of hypersonic and long-range strike weapons, and cited the need to strengthen the resiliency of space capabilities and directed energy weapons to counter these developments.

Lastly, Dr. Davis addressed the issue of civil-military fusion. He said while it is known that civil-military fusion is important given that the private sector is leading the development of emerging technologies, the traditional procurement system once again poses as an obstacle. He raised the question of whether democracy or authoritarianism is advantageous for civil-military fusion.

Dr. Raska made a presentation titled "Defense Innovation and the Future of Conflicts in East Asia." First, he discussed what changes have taken place. Dr. Raska stated that the security environment in East Asia has become ever more complex, and that existing major flashpoints have become increasingly interconnected, embedded in the strategic competition between the U.S. and China. Furthermore, he expressed the view that the relationship between technology, innovation, and national strength is changing, namely, innovation through revolutionary technology has become a source of national strength, resulting in a race for technological dominance between not only the U.S. and China but also among many countries and bringing an end to the West's hegemony over emerging technologies. In addition, he noted that the starting point for innovation in emerging technologies has shifted to the private sector rather than the military, and thus the competition over technology is also a contest for the ability to use private sector technology for military purposes. Dr. Raska refers to the ongoing military transformation with these characteristics as "AI RMA (Revolution in Military Affairs)," arguing that its context is similar to previous transformations but that the actual characteristics differ from before. In this context, he explained that Singapore is also transforming its military, motivated not only by the aforementioned security environment but also by domestic circumstances, such as the declining birthrate, as well as the country's desire to increase strategic independence by reducing technological dependence on foreign countries. Lastly, Dr. Raska pointed out that the nature of warfare is likewise changing, noting that automated warfare, featuring heavy use of high-tech capabilities such as human-machine

teaming and cyber capabilities, will coexist with new forms of hybrid or gray zone conflicts that mainly use low-tech military capabilities.

Secondly, Dr. Raska discussed what has not changed. Specifically, he noted that the uncertainty and complexity of war, which Carl von Clausewitz termed as fog and friction, will remain; that the effects of new innovations are relative to the capabilities of the opponent and therefore the cycle of evolving technological, operational, and organizational countermeasures will repeat itself; and that it is humans who control technology and humans will continue to make the decision to resort to war.

Lastly, Dr. Raska discussed what should change. He stated that measures should be taken in leveraging innovation, such as providing incentives to use previously underutilized resources such as universities and the private sector. He also pointed out the need for institutional agility in the bureaucracy, noting that faster and more creative use of innovation depends on the ability to embrace change by the government bureaucracy. He concluded that it is important to address the international governance of emerging technologies to ensure competition over technology does not go out of control.

Dr. Danilin gave a presentation titled "Beyond Technology: Political Economy of the U.S.-China Digital Conflict and Its Global and Regional Implications." Dr. Danilin began by providing an overview of the market conditions of information and communication technologies (ICT), explaining that a small number of countries account for a considerable share of this global market. He pointed out that there is significant division of labor and interdependence in the ICT industry supply chain, noting that China's ICT industry with a rapidly growing presence is heavily dependent on imports of high-tech components from the U.S. and other countries and that the U.S. still has superiority in the number of citations in cutting-edge technical papers and so on. He perceived that China is still on the path to becoming a leader in research and technology. China's leadership is concerned about this dependence and aims to restructure the global value chain and gain advantage in future markets under techno-nationalism. Dr. Danilin pointed out that such behavior is not unique to China and that it is shared more or less by emerging economies.

Dr. Danilin explained that the U.S. response to China's digital rise dates back to the mid-2010s, i.e., it did not begin during the Trump administration and still continues in the Biden administration. He discussed that the strategic containment of China is supported by several logics, such as defense, economic security, and politics, which in turn make this policy sustainable. He then stated that the U.S. measures are familiar ones that have been seen in the past. At the same time, he pointed out that similarity with past

cases is limited as the situation of the U.S.-China confrontation is different from that of the technological competition between the U.S. and the Soviet Union or between Japan and the U.S., which was biased toward either the military or the economy.

Dr. Danilin noted that the political economy of the ongoing technology competition is characterized by a strong logic to securitize digital technology. That is, the discourse of technological innovation, combined with geopolitics and domestic conditions, has led to the perception of digital and high-tech markets as "strategic resources," to the interpretation of emerging technologies as crucial structural and institutional power, and to the use of the actions of companies and others as tools for projecting power.

Lastly, Dr. Danilin discussed the global and regional impacts of such technology war. He viewed that the perception of digital technology as part of a non-cooperative game will increase the likelihood of conflict and create blocs that will force countries to decide which of the conflicting camps to join. At the same time, he pointed out that ICT technology and the Internet market cannot be completed in a single country, making globalization inevitable, and expressed hope that this will provide a type of buffer against geopolitical conflict.

In the Session 2 discussion, discussant Mr. Akimoto asked the following questions regarding the three presentations. He asked Dr. Davis about the implications for the technology innovation policies of AUKUS and QUAD, Dr. Raska about the future of the technology innovation ecosystem and prospects for international cooperation, and Dr. Danilin about the implications of the "Thucydides' trap" (a metaphor mentioned in his presentation) in the technology competition.

Dr. Davis stated that the key domain where AUKUS will bear fruit most quickly, before the submarines to be deployed in the 2030s, is R&D of quantum, AI, cyber, hypersonic, and other emerging technologies. He noted that QUAD also offers more room for cooperation on R&D of dual-use emerging technologies than traditional military cooperation, and conveyed the importance of deepening cooperation between AUKUS and QUAD on these common tasks. Citing the ongoing U.S.-Australia technical cooperation on unmanned underwater vehicles as an example, Dr. Davis noted that the impacts of developing such emerging technologies and their implementation in the defense sector should be considered, specifically, the impacts on postures based on traditional equipment requiring deployment time, such as submarines.

Dr. Raska noted that developing future defense capabilities solely in cooperation with the traditional defense industry will become difficult in a region like East Asia, where interstate security rivalries and economic interdependence coexist and the security

environment could change dramatically with rapid technological innovation. For this reason, he stressed the need for defense authorities in each country to strive to build relationships with startups and other emerging players and create a collective defense innovation ecosystem that transcends the traditional defense industry. In this regard, Dr. Raska highlighted the critical importance of institutional and organizational foundations that will enable defense authorities to absorb and apply innovative technologies and ideas flexibly and quickly.

Dr. Danilin responded that the "Thucydides' trap" metaphor refers to a situation in which techno-nationalism amidst the U.S.-China competition or the competition between democracy and authoritarianism spills over into global market activities for high-tech technologies, making mutual cooperation and negotiations (for the pursuit of economic gain and the R&D of high-tech technologies) impossible. While the present U.S.-China technological competition debate tends to emphasize the superiority in emerging technologies as the source of national competitiveness, he noted that on the contrary it is necessary to understand the negative aspects of the current competition as described above.

Chapter 1
The Emergence of Decision-Centric Warfare

Bryan Clark

The US Department of Defense (DoD) increasingly focused its doctrine and capability development during the past decade on great power opponents such as the People's Republic of China (PRC) and Russian Federation or nuclear-armed regional powers like North Korea. The most stressing campaigns US forces could face against these adversaries dominated DoD planning, with the assumption that worst-case scenarios also capture the needs for "lesser-included" cases.[1] Recognizing DoD's focus on high-intensity warfighting, however, adversaries are methodically developing strategies and systems that circumvent the US military's strengths and exploit its vulnerabilities by avoiding the types of situations for which US forces have prepared.[2]

As part of their efforts to asymmetrically counter US military strengths, operational approaches being pursued by the PRC and Russian militaries share an emphasis on information and decision-making as the main battlegrounds for future conflict. Concepts such as the People's Liberation Army's (PLA) System Destruction Warfare or the Russian military's New Generation Warfare direct forces to electronically and physically attack an opponent's ability to obtain accurate information while introducing false data that erodes the defender's ability to orient. Simultaneously, the aggressor's military and paramilitary forces isolate or attack targets without escalating the conflict in ways that could provide a pretext for large-scale US and allied military retaliation.[3] The dilemmas posed by degraded information and an inability to employ traditional US military responses could enable aggressors to achieve their objectives without resorting to attrition as the primary success mechanism.

---

1 Eric Larson, "Force Planning Scenarios, 1945–2016: Their Origins and Use in Defense Strategic Planning," (Santa Monica, CA: RAND, 2017), https://www.rand.org/pubs/research_reports/RR2173z1.html.

2 Kilcullen, David. The Dragons and the Snakes: How the Rest Learned to Fight the West. United States: Oxford University Press, 2020.

3 James Derleth, "Russian New Generation Warfare: Deterring and Winning at the Tactical Level, *Military Review,* September/October 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Derleth-New-Generation-War/.; Jeff Engstrom, *Systems Confrontation and System Destruction Warfare* (Santa Monica, CA: RAND, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.

Decision-centric concepts like those pursued by the PRC and Russian governments will likely be a significant form of future conflict, especially as more confrontations occur outside the context of large-scale existential combat. When a government's survival is at stake, its leaders would be more likely to adopt attrition-based approaches in an attempt to avoid defeat. Although decision-making and information would remain important when a conflict becomes attritionary, the lethality and survivability of individual units could be equally decisive.

During the late Cold War, the US military's revolutionary approach to precision-strike warfare leveraged the then-new technologies of communication datalinks, stealth, and guided weapons. Similarly, decision-centric warfare may be the most effective way to militarily exploit artificial intelligence (AI) and autonomous systems, which are arguably today's most prominent technologies. An example of this approach is the Defense Advanced Research Projects Agency's (DARPA) Mosaic Warfare concept, which combines AI-enabled command and control (C2) with forces that achieve greater disaggregation than today's US military by incorporating a larger proportion of autonomous systems.

Mosaic Warfare's central idea is that disaggregated manned and autonomous units guided by human command with AI-enabled machine control could use their adaptability and apparent complexity to delay or prevent adversaries from achieving objectives while disrupting enemy centers of gravity to preclude further aggression.[4] This approach is consistent with maneuver warfare, and contrasts Mosaic Warfare with attrition-based strategies employed by Allied forces during the Second World War and by the US military during post-Cold War conflicts in Kosovo, Iraq, and Libya. Although Mosaic Warfare employs attrition as part of creating dilemmas for enemies, its primary mechanisms to achieve objectives are denying, delaying, or disrupting adversary operations rather than eroding an opponent's military power to the point where it can no longer fight effectively.

Although they share a common foundation, Mosaic Warfare builds on maneuver warfare by proposing a force design and C2 process that would enable the US military to execute a larger and more diverse set of courses of action (COA) compared to an opponent. In a decision-centric confrontation, the force with such an "optionality advantage" would be more likely to impose an insoluble combination of dilemmas on

---

4 For more details on Mosaic Warfare, see Bryan Clark, Dan Patt, and Harrison Schramm, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*, (Washington, DC: Center for Strategic and Budgetary Assessments, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations.

the adversary.[5]

Mosaic Warfare would also differ with maneuver warfare in terms of its scope and timeframe. Whereas maneuver warfare is viewed as a tactical and operational-level military concept, Mosaic Warfare's force design and C2 approach would yield optionality advantages at the strategic level as well as in the development and fielding of new capabilities before a confrontation begins.

Force Design

The US military is already adopting many of the elements of mosaic force design. To increase optionality, mosaic force design would replace a portion of the US military's monolithic, self-contained platforms and units with a larger number of smaller, less-expensive, and less multifunctional units and systems. Although these smaller units may have less endurance, self-protection, or capacity than the elements of today's force, they could be deployed or escorted into theater by multimission platforms and considered attritable or expendable in combat. Figure 1 shows how a mosaic design approach could be implemented in the US Navy's force structure, which increases the overall number of vessels without growing procurement or sustainment costs.[6] The Navy and other US military services are already moving in the direction of more distributed force structures that are consistent with mosaic force design.[7]

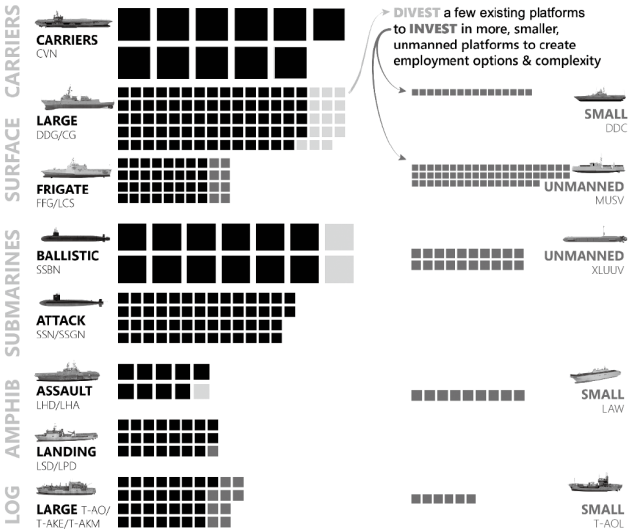
---

5 Robert Leonhard, The Art of Maneuver: Maneuver Warfare Theory and AirLand Battle (New York: Ballantine Books, 1991), pp. 66–74.

6 Bryan Clark, Timothy A. Walton, and Seth Cropsey, *American Sea Power at a Crossroads: A Plan to Restore the US Navy's Maritime Advantage*, (Washington, DC: Hudson Institute, 2020), https://www.hudson.org/research/16406-american-sea-power-at-a-crossroads-a-plan-to-restore-the-us-navy-s-maritime-advantage.

7 Ben Werner, "SECNAV Modly Says Nation Needs Larger, Distributed Fleet of 390 Hulls," *USNI News,* February 28, 2019, https://news.usni.org/2020/02/28/secnav-modly-says-nation-needs-larger-distributed-fleet-of-390-hulls.

Figure 1: Example of how the US Navy could be rebalanced to implement Mosaic Warfare force design principles



The current and proposed future force cost approximately the same amount to buy and operate, incorporating inflation.
Source: Adapted from Bryan Clark, Timothy A. Walton, and Seth Cropsey, *American Sea Power at a Crossroads: A Plan to Restore the US Navy's Maritime Advantage*, (Washington, DC: Hudson Institute, 2020), https://www.hudson.org/research/16406-american-sea-power-at-a-crossroads-a-plan-to-restore-the-us-navy-s-maritime-advantage

The greater number and diversity of units in a mosaic force would provide more potential combinations to commanders, allowing them to identify acceptable COAs faster and more easily select COAs that have a higher probability of success. The mosaic force's disaggregation would also enable commanders to calibrate the capacity and capability of force packages more precisely, which could allow a force to be spread over a larger number of simultaneous tasks compared with today's US military. From an opponent's perspective, the mosaic force's higher decision-making tempo, scale, and effectiveness compared to a traditional force would tend to foreclose more of the opponent's COAs, further strengthening the mosaic force's optionality advantage.

Rebalancing US forces toward a larger number of smaller platforms and formations creates operational benefits. The more disaggregated mosaic force would be better able to mount feints, probes, and other high-risk, high-payoff operations that would not be worth the potential loss of a monolithic, multi-mission platform or formation.

Disaggregation would also enable more force package options that can proportionally counter gray-zone or sub-conventional aggression. In contrast, today's US gray-zone responses either employ small numbers of expensive platforms at high risk of being overwhelmed adjacent to an adversary's territory, or larger formations that can protect themselves but are likely disproportionate to the situation.[8]

Across a longer competition, the smaller, less-multifunctional units in the mosaic force could more easily incorporate new mission systems and technologies compared to their monolithic, multimission counterparts. As a result, the mosaic force could adapt more quickly compared to today's military by promptly fielding new sensors, radios, weapons, or electronic warfare systems as they emerge from research and development instead of waiting for costly and time-consuming integration.[9]

C2

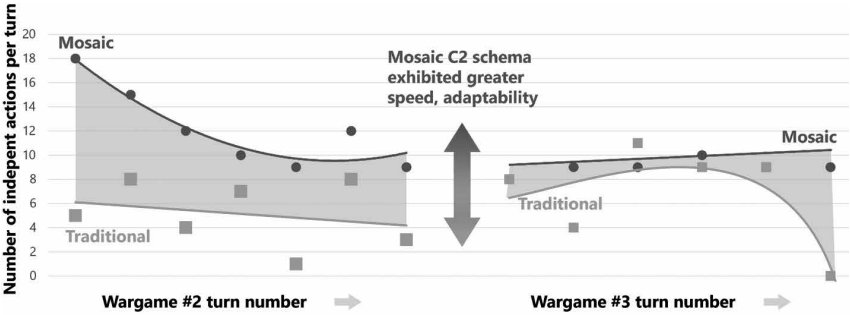
The staff-managed and doctrine-driven C2 process of today's military is too slow and lacks the capacity to rapidly develop COAs that integrate a large number of disaggregated units in performance of changing missions. The mosaic C2 approach addresses the shortfalls of staff-driven planning by combining human command with machine control, in which human commanders identify tasks, set constraints and priorities, and identify forces available for use; machine-enabled decision support systems then develop proposed COAs that support the commander's intent. Together, a more disaggregated force and a machine-enabled C2 process would enable faster decision-making at scale, as evidenced in the wargame performance of mosaic teams shown in Figure 2.

---

8 Zachary Cohen and Ryan Browne, "US B-52 bomber flies near contested islands in South China Sea," CNN, March 5, 2019, https://www.cnn.com/2019/03/05/politics/us-b-52-bomber-training-south-china-sea/index.html; Geoff Ziezulewicz, Two US aircraft carriers are operating in the South China Sea; Air Force B-52 joins them." July 6, 2020, https://www.navytimes.com/news/your-navy/2020/07/06/two-us-aircraft-carriers-are-operating-in-the-south-china-sea-air-force-b-52-joins-them/.

9 These benefits are detailed in Bryan Clark, Dan Patt, and Harrison Schramm, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations*.

Figure 2: Comparison of task completion between mosaic forces and traditional military forces in recent wargames



Wargames suggest that a Mosaic C2 approach combined with a more disaggregated force structure can yield faster, more adaptable operations.
Source: Bryan Clark, Dan Patt, and Harrison Schramm, Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations.

Human command and machine control would also support the US military concept of mission command, in which subordinate leaders rely on their own initiative and creativity to pursue the intent of senior commanders when communications are lost.[10] As US forces become more disaggregated or distributed, junior commanders will be less able to creatively employ units and systems under their control without planning staffs. As a result, junior commanders cut off from headquarters could fall back on habit or tactics that are predictable by the enemy. Decision support systems would avoid this loss of optionality by enabling junior commanders to effectively improvise and create unexpected COAs when communications are degraded.

[10] Mission Command: C2 of Army Forces, US Department of the Army, 2020, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN19189_ADP_6-0_FINAL_WEB_v2.pdf.

Implementing Decision-Centric Warfare

DoD's C3 efforts today are organized under its Joint All-Domain C2 (JADC2) strategy,[11] which includes the US Air Force's Advanced Battle Management System (ABMS),[12] the Army's Project Convergence,[13] and the Navy's Project Overmatch.[14] System development under JADC2 has largely focused on communications to connect a greater variety of disparate units via ABMS, but gaining a decision-making advantage will require that commanders go beyond merely connecting forces to also develop COA and compose force packages faster or more effectively than their opponents.[15]

Although JADC2 should help commanders communicate with a more diverse and dynamic set of forces, the current staff-driven US military planning approach will be unable to review the growing range of possible COAs at an operationally relevant tempo. To speed up planning, staffs are likely to fall back on doctrine or habit that an enemy would more easily predict, reducing the decision advantage of US forces.

Some new technologies are needed to enable DoD's emerging force designs, such as autonomous vehicle controls, network management systems, and small form-factor sensors or effectors. However, these efforts are well-supported and reaching a high level of maturity. Given DoD's progress on fielding more disaggregated forces, C2 should be the focus of technology development for decision-centric warfare in general and Mosaic Warfare in specific. The technology for human command and machine control is already emerging from DoD initiatives designed to support specific military missions such as air-to-air combat or missile defense.[16] C2 technology development will need to build on these programs and enable management of an entire force across multiple missions

---

[11] Theresa Hitchens, "Exclusive: J6 Says JADC2 Is A Strategy; Service Posture Reviews Coming," *Breaking Defense,* January 4, 2020, https://breakingdefense.com/2021/01/exclusive-j6-says-JADC2-is-a-strategy-service-posture-reviews-coming/.

[12] Theresa Hitchens, "ABMS Demo Proves AI Chops For C2," *Breaking Defense*, September 3, 2020, https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

[13] Mark Schauer, "Project Convergence a generational shift for Army," US Department of the Army, October 7, 2020, https://www.army.mil/article/239770/project_convergence_a_generational_shift_for_army.

[14] David Larter, "The US Navy's 'Manhattan Project' has its leader," *C4ISRNet*, October 14, 2020, https://www.c4isrnet.com/naval/2020/10/14/the-us-navys-manhattan-project-has-its-leader/.

[15] John Hoehn, "Joint All Domain C2 (JADC2)," Congressional Research Service, September 28, 2020, https://fas.org/sgp/crs/natsec/IF11493.pdf.

[16] DARPA, "AlphaDogfight Trials Go Virtual for Final Event," DARPA, August 6, 2020, https://www.darpa.mil/news-events/2020-08-07; Jen Judson, Inside Project Convergence: How the US Army is preparing for war in the next decade," Defense News, September 10, 2020, https://www.defensenews.com/smr/defense-news-conference/2020/09/10/army-conducting-digital-louisiana-maneuvers-in-arizona-desert/.

against adversaries that are actively attempting to undermine US decision-making.

In contrast to the playbooks and tactics used in today's operational planning, realizing the greater optionality inherent in the mosaic force design will require decision support systems that can rapidly analyze numerous potential COAs and adversary responses, providing commanders an assessment of each COA's likelihood of success and how it may impact the opponent's decision space. Perhaps most importantly, C2 tools for decision-centric warfare will need the ability to develop and consider COAs outside the bounds of previous engagements or doctrine to surprise an opponent with an unexpected action or respond to an unlikely enemy operation. Some DoD programs are already pursuing the algorithms needed to support this approach to "changing the game" on an opponent.[17]

Over a longer conflict, C2 tools will also need to help commanders understand how they can orchestrate individual engagements to implement their strategy and maintain an optionality advantage. For example, a commander can initially use a large number of simultaneous operations, including numerous feints and probes, to overwhelm enemy decision-making and narrow decision space. Using the information gained from their opening actions, US forces could then execute a focused set of attacks against primary targets while pursuing suppression operations against enemy forces using attritable units with a high likelihood of loss. The US commander could close the mission by mounting a series of unexpected COAs against remaining targets to constrain the enemy's options and keep it off balance until the US force accomplishes its objectives. A decision-centric C2 tool should aid commanders in considering a series of COAs like these against a range of enemy responses.

Forces conducting decision-centric warfare will require a complex set of C2 and communications capabilities to fully exploit the optionality possible with a more disaggregated force design and narrow the COAs available to opponents. These mission integration capabilities are described in the next section.

Integrating heterogeneous military forces

Advancements in communication technology, modularized electronics, and software-defined systems are propelling explosive growth and specialization across most sectors

---

[17] DARPA, "Gamebreaker AI Effort Gets Under Way," DARPA.mil, May 12, 2020, https://www.darpa.mil/news-events/2020-05-13.

of the US economy. Driven by technology companies' business models, consumers can obtain increasingly tailored products and services, often delivered directly to their homes. Although accelerated by 2020's coronavirus pandemic and the exigencies of remote work, these developments reflect underlying trends that are inexorably leading toward a future of diverse products and services being delivered to rapidly expanding markets.[18]

Military forces are also evolving toward a combination of heterogeneity and scale. The DoD is pursuing greater resilience through distributed force structures intended to grow the number of targets an enemy would need to engage and expand the variety of ways US forces could conduct offensive operations.[19] In a fiscally constrained environment, further distributing the US military will necessarily increase its heterogeneity. If today's US joint force was distributed into a larger number of units having approximately the same capability and capacity, either the overall US military would be too small because each unit would be a costly multimission platform or formation, or DoD would lack needed high-end capabilities such as air defense or long-range fires that are too expensive to be carried by every unit. Therefore, compared to the current US military, DoD's future force design will likely be more disaggregated and heterogeneous, combining fewer large, multi-mission platforms and troop formations with a larger number of smaller, more specialized, units.

In addition to the improved resilience arising from distribution, a more heterogeneous US force will likely be more effective in confrontations where success results increasingly from information and decision superiority rather than attrition. For example, the Mosaic Warfare concept contends a military able to exploit heterogeneity at scale could gain a decision-making advantage over opponents by affording commanders greater adaptability and creating more complex presentations for the enemy to assess,

---

[18] Scott Galloway, Post-Corona, (New York, NY: Penguin/Random House, 2020), pp. 16-24.

[19] Office of the Chief of Naval Operations, Deputy Chief of Naval Operations (Warfighting Requirements and Capabilities - OPNAV N9), "Report to Congress on the Annual Long-Range Plan for Construction of Naval Vessels," (Washington, DC: US DoD, 2020), p. 9, https://media.defense.gov/2020/Dec/10/2002549918/-1/-1/1/SHIPBUILDING%20PLAN%20DEC%2020_NAVY_OSD_OMB_FINAL.PDF; Charles Q. Brown, "Accelerate Change, Or Lose," US Department of the Air Force, August 2020, https://www.af.mil/Portals/1/documents/csaf/CSAF_22/CSAF_22_Strategic_Approach_Accelerate_Change_or_Lose_31_Aug_2020.pdf; Headquarters, US Marine Corps, "Force Design 2030," US Department of the Navy, March 2020, https://www.hqmc.marines.mil/Portals/142/Docs/CMC38%20Force%20Design%202030%20Report%20Phase%20I%20and%20II.pdf?ver=2020-03-26-121328-460; Jen Judson, "US Army's $7 billion wish list would boost multidomain units and wartime funding," *Defense News*, February 21, 2020, https://www.defensenews.com/smr/federal-budget/2020/02/21/armys-7-billion-wish-list-would-boost-mutlidomain-units-and-wartime-funding/.

understand, and defend.[20]

A contemporary example of mosaic-like force design is US Special Operations Forces (SOF), which consist predominantly of small, specialized units supported by a few multimission platforms or troop formations. However, the SOF model for training, equipping, and planning would be too expensive and time-consuming to apply across the entire US military. Enabling greater adaptability and composability by DoD's general-purpose forces within likely fiscal and organizational constraints will require new approaches to force management and preparation that balance scalability with the goal of providing more options to commanders.

Decision-centric warfare implies two levels of competition. Operationally, militaries will need the ability to exploit the adaptability possible with more distributed and heterogeneous forces by recomposing and integrating forces in the field. Institutionally, militaries will need to compete by evolving capabilities over time through the adoption of new technologies and concepts that exploit emerging opportunities or address new threats and challenges.

Heterogeneity at scale would improve the US military's composability, but decision superiority will depend as much or more on C3 capabilities that integrate units and coordinate their operations. In addition to the difficulty of organizing more numerous and diverse military units, today's planning and management processes are likely to be overwhelmed by the complexity created by the greater variety of possible force compositions and effects chains inherent in a more disaggregated force. New C3 organizations, processes, and systems will therefore be needed to implement decision-centric warfare regardless of the level of heterogeneity eventually achieved by the US military.

Framed another way, merely establishing machine-to-machine communications across the existing force is unlikely to deliver an asymmetric advantage against adversaries. And while networking everything all the time is a noble long-term goal it is impractical for the foreseeable future. A more fertile competitive field will be managing the timing and orchestration of force combinations possible with the units that commanders can communicate with to pursue immediate, focused military objectives. Decision support tools could help commanders understand their communications availability and harness

---

[20] Bryan Clark, Dan Patt, and Harrison Schramm, *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems for Decision-Centric Operations* (Washington, DC: CSBA, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations.

the complexity of a more heterogeneous force that embodies a greater variety of potential force packages and COAs. The US military is already expanding its use of computer based C2 aids, some of which employ artificial intelligence (AI), to speed the development and improve the effectiveness of COAs using modeling and simulation and the results of previous operations.[21]

The construct DoD normally uses to assess needs associated with new operational approaches considers doctrine, organization, training, material, leadership, personnel, and facilities (DOTMLPF). Because the doctrine for Mosaic Warfare, JADC2, and the joint warfighting concept are already under development, this study will focus on the remaining DOTMLPF elements, organized into three main categories: mission integration, operational infrastructure, and institutional processes.

Mission Integration

Today force composition is largely performed by the military services, which organize, train, and equip units that are then deployed to Combatant Commanders (CCDR) and their domain-specific service component commanders.[22] DoD's reliance on services to create force packages, however, can constrain the variety of compositions to those using a single service's capabilities. Moreover, services are incentivized to limit the variety of force packages they create to contain costs associated with preparing and certifying units before deployment.

To exploit the potential of a more heterogeneous and recomposable military, CCDRs will need mechanisms in theater to recompose and integrate forces from multiple services and domains. However, identifying when recomposition is warranted will require ongoing assessment of current force packages' effectiveness and adaptability across a range of potential situations the CCDR could need to address. Integrating new force packages in theater will also incur costs in terms of operational infrastructure such as logistics, protection, transportation, and C3 capabilities. To manage the scope and cost of their assessments and recomposition efforts, CCDRs could focus on a small set of operational challenges that must be tackled to enable their plans for deterrence and warfighting preparation. A mission integration cell on the CCDR staff could continuously

---

[21] Mallory Shelbourne, "Services Looking for 'Synergy' in JADC2 Efforts," *USNI News*, November 13, 2020, https://news.usni.org/2020/11/13/services-looking-for-synergy-in-jadc2-efforts.

[22] The joint force component commanders associated with most combatant commanders are air, maritime, and land.

evaluate the ability of available forces to address the CCDR's operational challenges and direct the recomposition of forces in theater when the improvement in effectiveness and adaptability outweighs the costs associated with operational infrastructure.

The process of mission integration will also yield insights that should be applied to future capability development. Through their assessments, mission integration cells may discover potential new capabilities that would yield a substantial improvement in effectiveness or adaptability compared with current approaches to an operational challenge. To act on these opportunities, DoD will need to leverage a federated model of capability development encompassing service program offices, rapid capability organizations, and "mission factories" such as Navy and Air Force warfare centers.[23]

Operational Infrastructure

Realizing the greater potential optionality of a more heterogeneous future force will depend on changes to the nature and provisioning of military transportation, protection, logistics, energy, C2, and communications infrastructure. Smaller specialized units such as patrol vessels, unmanned aircraft, or troop formations at the battalion level and below will often need to be carried into theater and afforded more inorganic support and protection than larger self-contained multimission platforms and formations. In some cases, multimission units could operate in concert with smaller, more specialized forces to provide protection and support. When operating independently, less-multifunctional troop formations and manned or unmanned platforms may need more disaggregated support infrastructure and logistics forces compared to today's efficient, but centralized, supply and fuel depots, aircraft, and ships.

Military capabilities that are less geographically constrained, like space-based sensing and communications systems or information and cyber tools, will also need to be integrated by CCDRs into recomposed force packages. Like smaller, more specialized platforms and formations, these capabilities may also depend on operational infrastructure; cyber tools may need transportation for physical access to targets or a commercial satellite sensor may depend on interoperability software to connect with an unmanned military surface vessel.

---

[23] See US Air Force, U.S. Air Force Warfare Center, Nellis Air Force Base, October 26, 2016, https://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284150/us-air-force-warfare-center/; US Navy, "Warfare Centers," US Naval Sea Systems Command, https://www.navsea.navy.mil/Home/Warfare-Centers/Who-We-Are/.

As noted above, mission integration cells will need to consider operational infrastructure in their analysis of new force compositions. The smaller, less multi-functional units in a more heterogeneous military force will not be able to meet all their own support requirements, necessitating operational infrastructure to be integrated into the new force packages that CCDRs create in theater.

DoD Institutional Processes

The forecast-based and supply-focused analysis, resource allocation, and capability development processes used today by DoD are ill-suited to realize the force design and C3 architectures needed to implement decision-centric warfare. Most significantly, a more recomposable force will not result in predictable system-of-system instantiations that can be used to identify capability gaps and deterministically define requirements for engineers to pursue through research and development (R&D). DoD will need new approaches to assess and satisfy its capability needs that reflect the greater optionality of a decision-centric force.

Today, the Joint Capabilities Integration and Development System (JCIDS) is designed to identify system requirements by forecasting the performance of planned capabilities in predicted future scenarios.[24] This approach depends on assumptions regarding the configuration of US forces, but as the US military becomes more recomposable, the specific combination of units and their tactics will be less certain. To assess the future US force's effectiveness, DoD could instead evaluate all the reasonable combinations of units that could be pursued in a realistic range of situations. The distribution of the force's effectiveness across configurations and scenarios can be represented as a statistical distribution, rather than the current point solution directed through JCIDS.

DoD is making some progress toward identifying requirements for composability through mission thread analysis and mission engineering.[25] The Office of the Secretary

---

[24] U.S. Joint Staff, "Charter of The Joint Requirements Oversight Council (JROC) and Implementation of The Joint Capabilities Integration and Development System (JCIDS)," CJCSI 5123.01H, 2018, pp. D-1–D-3, available at http://acqnotes.com/wp-content/uploads/2018/11/CJCSI-5123.01H-Charter-of-the-Joint-Requirements-Oversight-Council-JROC-and-Implementation-of-the-JCIDS-31-Aug-2018.pdf;

[25] See Statement by Ms. Barbara McQuiston to the U.S. Senate Appropriations Committee Subcommittee on Defense Innovation and Research April 13, 2021 or the DoD Mission Engineering Guide found at https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

of Defense (OSD), US Joint Staff, and military services are beginning to use this methodology. As applied today, mission thread analysis examines the information and data flows necessary to complete a specific kill chain against a target, which can expose gaps in data transfer and sharing that are not reflected in simplistic operational architecture illustrations. However, by assuming a static arrangement of force elements, DoD's current mission engineering efforts risk creating brittle systems-of-systems that only work in a single configuration. An asymmetric US advantage should flow from the ability to rapidly decompose and recompose forces and create new systems-of-systems combinations.

During the last decade, the US Congress and DoD established new acquisition processes that could improve the US military's ability to develop capabilities based on emerging technical opportunities and operational challenges rather than predictions of future needs.[26] However, DoD's ability to start, stop, or change course on capability development is fundamentally constrained by supply-based government budgetary structures and processes that are built around programs, rather than missions or demands, and require years to alter funding allocations. New budgeting mechanisms with more flexibility, such as mission-based budgeting or DoD's recent pilot on software appropriation, will be needed to address CCDR operational challenges by modifying or introducing new capabilities that assessments suggest could improve the force's effectiveness or adaptability.[27]

Conclusion and recommendations

Emerging technologies and new use cases are driving consumer products, services, and military forces toward a combination of heterogeneity and scale. In commercial applications, the Internet, mobile communications, modular products, and algorithm-enabled transportation are enabling the dispersion of tailored products and services to users. Military forces are able to similarly exploit networks, C2 tools, modular mission systems, and operational infrastructure to compose force packages that provide a

---

[26] Office of the Under Secretary of Defense for Acquisition and Sustainment, "DOD INSTRUCTION 5000.02: Operation of The Adaptive Acquisition Framework," January 23, 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093.

[27] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Budget Activity (BA) "BA-08": Software and Digital Technology Pilot Program," Defense Acquisition University, September 28, 2020, https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/SW%20APPROPRIATION%20BA-08%20FAQ.pdf.

combination of effectiveness and adaptability to CCDRs.

Whereas many commercial technology companies built their businesses around the ability to deliver bespoke products and services to widely distributed customers, DoD has largely been a bystander to the trend toward heterogeneity at scale. Although the Pentagon established a growing variety of capability development organizations and acquisition pathways to field more diverse systems faster, the goal of these efforts was to get capabilities more quickly to the warfighter rather than change its force development paradigm to harness fundamental technology trends.

The US military needs operational and institutional decision-making advantages to effectively deter opponents such as the PLA or Russian Armed Forces. Operationally, achieving a larger decision space depends on having military units and decision support tools able to compose force packages that are effective in a wide range of situations. Strategically, DoD's institutional processes will need new metrics and analytic approaches, more agile resource allocation structures, and a more responsive defense industrial ecosystem to adapt its capabilities for operational advantage.

As a first step, DoD should more proactively exploit the evolution of defense technology by explicitly adopting a federated model for mission integration. Today's approach of services integrating deploying units and affording CCDRs little ability to recompose force packages in theater denies US commanders their most effective opportunity for adaptation and fails to leverage ongoing advances in networking and interoperability. In addition to yielding greater operational optionality, providing CCDRs the tools and operational infrastructure to compose forces would also enable feedback for capability developers that are already organizing along the lines of the mission factories, rapid capability organizations, and proposed in the section of Mission Integration.

To fully exploit the opportunities in heterogeneity at scale, DoD should go further and begin to reform some of its decision processes. By prioritizing adaptability and effectiveness as metrics for capability assessment, force planners could privilege systems that improve outcomes across a range of situations and base decisions on value instead of cost. Performing these assessments will require new methods and tools for analysis that can quickly examine many situations at a lower level of fidelity compared to today's deep analysis within a narrow set of canonical scenarios. And to provide CCDRs the operational infrastructure to integrate forces in theater or the new and modified capabilities needed to achieve acceptable effectiveness and adaptability, DoD will need budget categories with more flexibility than today's program element structure.

DoD will need to engage the defense industry as a partner in its effort to improve

operational and strategic agility. Technology and conceptual trends are driving commercial and defense ecosystems toward new models of delivering capability and engaging with the government as a customer. Measuring the utility of new capabilities based on value rather than cost, DoD may be able to incentive greater commercial contributions to defense capabilities.

The Pentagon should stop letting the evolution of technology pass it by. By embracing new models for capability development, integration, and decision-making, DoD could gain the organizational flexibility to compete effectively with its PRC and Russian counterparts. If it doesn't, the US military runs the risk of ending up like the IBM PC—a great capability for its time but disrupted into irrelevance by more agile competitors.

Chapter 2
The Impact of Emerging Technologies on the Strategic Environment of the Asia-Pacific Region: Focus on Japan's Perspective

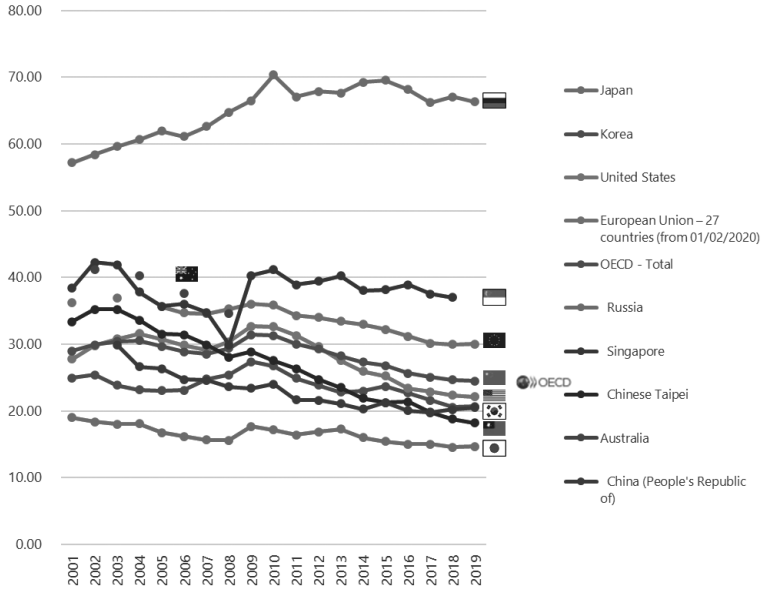
FUJITA Motonobu

1. Introduction

In recent years, investment in emerging technologies has increased in various countries, including Japan. Investments in emerging technologies are made by investing in research and development (R&D). According to the OECD's definition, "Research and experimental development (R&D) comprise creative and systematic work undertaken in order to increase the stock of knowledge – including knowledge of humankind, culture and society – and to devise new applications of available knowledge."[1] R&D investment is also defined by the Office of Management and Budget within the Executive Office of the President of the United States as "expenses included in the calculation of net costs to support creative and systematic work undertaken to increase the stock of knowledge and to use such knowledge and practical experience for devising new or improved products and processes, with the expectation of maintaining or increasing national economic productive capacity or yielding other future benefits."[2]

In the private sector, R&D investment is increasing year after year. In 2018, the top 1,000 companies leading global innovation alone invested $782 billion in R&D.[3] Profits are increasing for these companies. This shows that investment in R&D is positioned as a source of future competitive strength.

Figure 1: Percentage of Government expenditure to GERD



GERD: Gross Domestic Expenditure on R&D

On the other hand, the ratio of government R&D expenditure to total domestic R&D expenditure has been gradually declining in many countries, although the average for OECD countries is about 25%.[4] As for Japan, the ratio has been stable at about 15%. Based on this, we can consider governments to still be a major, although not dominant, player in R&D investment.

Beyond military means, there are various means of cross-national competition encompassing politics, economics, and the military. Technology has always played a central role in international politics, both in times of peace and in times of war.[5] Investment in technology leads to the building of military capabilities, but it is not practical to invest equally and fully in all areas of technology. Each country must thus weigh the relative importance of investment in technology. Therefore, investment in technology can be considered a statement of national intent.[6]

In this report, I endeavor to clarify Japan's perspective on the impact of investment in emerging technologies on the strategic environment of the Asia-Pacific region.

2. Definition of Emerging Technologies in this Report

There have been various attempts to define emerging technologies, but there is no clear and consistent definition.[7] Some believe that the term simply refers to technologies in their budding stage,[8] while others focus on their importance from the perspective of export control,[9] others on their economic impact,[10] and others on the process of extending them to new areas of application.[11] For example, Section 232 of the U.S. National Defense Authorization Act for Fiscal Year 2020 defines emerging technologies as "technology determined to be in an emerging phase of development by the Secretary of Defense, including quantum computing, technology for the analysis of large and diverse sets of data (commonly known as 'big data analytics'), artificial intelligence, autonomous technology, robotics, directed energy, hypersonics, biotechnology, and such other technology as may be identified by the Secretary."[12] This report focuses on the impact of technology on the security environment and thus defines emerging technologies as technologies that can have an impact encompassing doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).[13]

3. The "Strategies-to-Tasks" Framework[14]

In order to consider the impact of emerging technologies on the strategic environment, it is necessary to clarify the perspective. The "strategies-to-tasks" framework developed at the RAND Corporation clarifies the correspondence between a series of objectives, from national security objectives to military task objectives. Specifically, it consists of four steps: national security objectives and national military objectives, national military objectives and campaign objectives, campaign objectives and operational objectives, and operational objectives and operational tasks. Such an approach avoids bias toward specific organizational objectives and tasks and brings consistency between the different objectives.

For a long time, R&D has been viewed as something to create the means to efficiently accomplish military tasks. Until the Cold War, national security goals were clear, and it was relatively easy for defense scientists and engineers to pursue R&D according to documented and clearly defined requirements specifications.[15,16] However, with the current accelerating changes in the security environment, there is always uncertainty in predicting future ways of war.[17,18] Thus, realizing requirements specifications for new equipment is not as easy as it used to be, and scientists and engineers now need to conduct R&D while being aware of the multiple hierarchies of the strategies-to-tasks

framework.

In this report, I use the strategies-to-tasks framework as a reference and analyze the impact of emerging technologies on the strategic environment from a broad perspective.

4. Basic Equipment Policy and Technology Policy of the Ministry of Defense (MOD)

Defense acquisition involves a long period of time, from the research phase to the procurement, maintenance, and operation of equipment. Foresight is essential for planned personnel allocation and capital investment, which requires a long period of time from investment to returns. Therefore, the MOD announced the Strategy on Defense Production and Technological Bases[19] in June 2014 in order to clarify the basic direction of its equipment policy and technology policy, and the Defense Technology Strategy[20] in August 2016 in order to clarify the basic direction of technological capabilities strengthening.

In this report, I explain Japan's basic perspective with particular focus on references to emerging technology initiatives among these strategy documents.

(a) Strategy on Defense Production and Technological Bases[19]

The Strategy on Defense Production and Technological Bases was formulated to newly indicate the direction for the maintenance and strengthening of defense production and technological bases, succeeding the basic guideline for production and development of defense equipment[21] (the so-called *kokusanka-hoshin* [guideline for indigenous development/production]) formulated in 1970. The goals and significance of the Strategy are encompassed in three points:

1. Ensure sovereignty of security
2. Contribute to latently enhance deterrence and maintain and enhance bargaining power; and
3. Contribute to advance domestic industry driven by highly sophisticated technology.

One of the characteristics of this Strategy is that, from the perspective of effectively and efficiently maintaining and strengthening defense production and technological bases, the policy is to select the most appropriate method for acquiring equipment according to the characteristics of the defense equipment, with the following basic

options: (1) domestic development, (2) international joint development and production, (3) licensed production, (4) utilizing civilian goods, and (5) imports. Among the various measures for this, the specific measures for R&D are: (1) formulating an R&D vision; (2) developing the ability to survey technological information, including advanced civilian technologies; (3) strengthening cooperation with universities and research institutes; (4) cooperating with and utilizing R&D programs, including those that cover dual-use technology; (5) funding advanced research with promising output for defense, and (6) strengthening cooperation with overseas organizations. The Strategy can be interpreted as indicating a policy of focusing on the engineering process from basic technology to equipment systems, noting the need for a medium- to long-term perspective in the R&D of defense equipment, and then showing interest in advanced civilian technologies and the transfer of those technologies to the defense sector.

(b) Defense Technology Strategy[20]

The Defense Technology Strategy was formulated with the objective of practically and effectively strengthening the technological capabilities that are the basis of Japan's defense capabilities. The National Security Strategy also states from the viewpoint of national security, Japan's high technological capabilities are the foundation of its economic and defensive powers, and that Japan needs to take measures to strengthen them by further promoting and nurturing technologies including dual-use technologies.

Unlike the Strategy on Defense Production and Technological Bases, which indicates the basic direction from the perspective of developing defense industry bases, the Defense Technology Strategy is characterized by its emphasis on strengthening technological capabilities which are the foundation supporting defense equipment, rather than on the defense equipment itself.

Thus, the Strategy defines the following two MOD technology policy objectives:

1. Ensuring technological superiority; and
2. Delivering superior defense equipment through effective and efficient R&D.

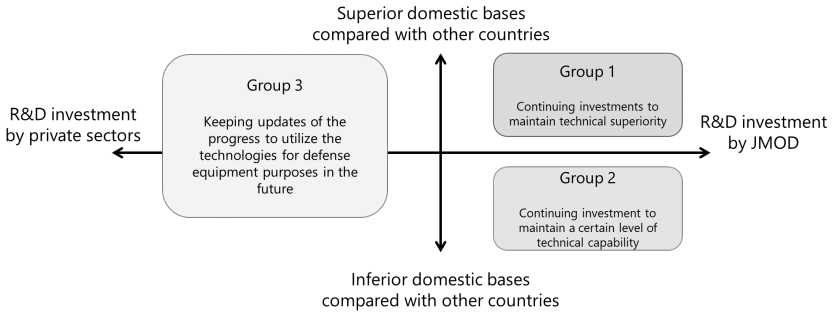
The objectives are considered to be complementary and synergistic, with no order of priority between them. By promoting them, the MOD intends to strengthen Japan's technological capabilities.

In order to achieve these objectives, the Strategy raises the following three measures to be taken by the MOD:

1. Technology Survey;

2. Technology Development; and
3. Technology Protection.

Figure 2: The three perspectives (or portfolios) in the Defense Technology Strategy



One of the characteristics of this Strategy is that it presents three perspectives (or portfolios) that should be considered as preconditions for promoting specific measures, taking into account the state of Japan's technology bases. In the Strategy, the MOD has laid out the three perspectives to be considered on four-quadrants, with the horizontal axis representing investment orientation (whether the MOD will actively invest) and the vertical axis representing the expected effects of investment (whether it is easy to achieve technological superiority), and has put forward basic investment policy for each group (Figure 2). The characteristics of each group and the basic investment policy are described below.

Group 1) Fields in which Japan already has superiority
Among the technologies referred to as emerging technologies, Group 1 can be considered to include those technologies in which Japan excels in and which have clear applications for defense. Examples include advanced material technologies that have received a certain level of recognition in international joint R&D. The MOD will continue to actively invest resources in these technology fields.

Group 2) Fields of technology in which Japan currently does not have a superior technological footing but which would put Japan at a strategic disadvantage if it does not maintain a certain level of technological capability

As is the case in many countries, the reason for investing in technology is not only to leverage strengths in some emerging technologies. The Strategy states that even for technologies in which Japan does not have a strategic technological footing compared to other countries, it will invest resources to maintain its technological capability because it may be at a strategic disadvantage if it does not maintain a certain level. Group 2 can be considered to include technologies that are not emerging technologies but rather those that are already at a mature stage. Furthermore, continuous investment in Group 2 technologies is considered important from the perspective of maintaining the defense equipment supply chain.

Group 3) Fields of technology where voluntary R&D is underway in the private sector
As shown in the previous figure, R&D investment in the private sector accounts for about 85% of R&D expenditures in Japan. The Strategy states that the MOD will not actively invest in fields of technology for which voluntary R&D is being conducted by the private sector because their applications for defense are not necessarily clear. However, the Strategy states that the MOD will keep track of technological trends in order to efficiently advance their conversion for defense equipment. In particular, Group 3 technologies are becoming increasingly important due to recent advances in digital technology.

Because understanding technological trends is, at the very least, the starting point for technology transfer to the defense sector, continuous and comprehensive research is essential. Going forward, it is expected that it will become increasingly necessary not simply to detect new technologies that are progressing in the civilian sector, but rather to transfer those technologies to the defense sector.[22] In other words, it will become increasingly necessary to review investments and processes aimed at building industry bases and clarifying defense requirements.

These are the basic directions of the current equipment policy and technology policy of the MOD. Various measures are currently being steadily implemented based on these strategies.

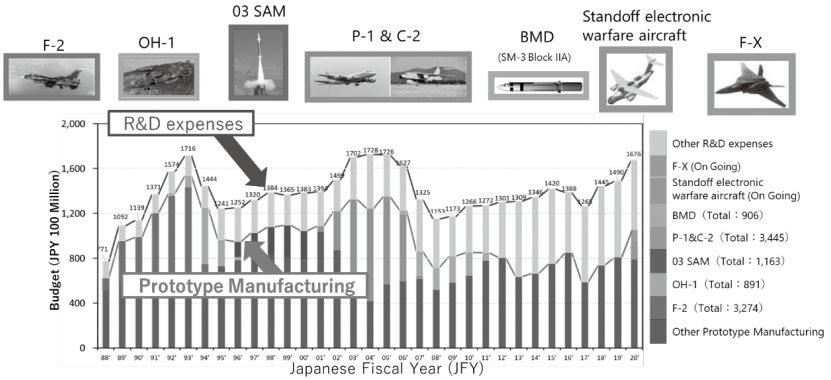
5. Trends in R&D Investment and Investment in Emerging Technologies by the MOD

The amounts and breakdowns of R&D investment are a useful clue for understanding a country's or organization's approach to investment in emerging technologies. Therefore,

this section discusses the trends in R&D investment based on the basic approaches for the equipment policy and technology policy of the MOD.

Figure 3 shows the changes in the MOD's R&D budget over the past 30 years. The horizontal axis represents the period 1988-2020, and the vertical axis shows the R&D budget and its breakdown. The colors of the bars respectively correspond to expenditures that include applied research[i] and test & evaluation,[ii] and expenditures for prototype manufacturing.[iii] The figure shows that R&D expenditures have fluctuated widely at the MOD in conjunction with specific big projects through now.

Figure 3: Changes in the MOD's R&D expenses



It is true that investment in specific big projects has played a certain role in achieving superior domestically produced equipment. However, Japan must decide whether to continue to prioritize investment in specific platform development in the future given the limited budget and time, or whether to balance medium- and long-term R&D investments and stably invest in acquiring and strengthening capabilities in the new domains of space, cyberspace, and the electromagnetic spectrum (EMS) without being biased toward a specific platform. Japan could also opt to allocate more resources in order to have a balance of both the aforementioned options. Because there has been no

---

[i] This can be interpreted as equivalent to 6.1 Basic Research, 6.2 Applied Research, and 6.3 Advanced Technology Development at the U.S. Department of Defense.

[ii] This can be interpreted as equivalent to 6.6 Test & Evaluation at the U.S. Department of Defense.

[iii] This can be interpreted as equivalent to 6.4 Advanced Component Development and Prototypes as well as 6.5 System Development and Demonstration at the U.S. Department of Defense.

noticeable change in the trend so far, it is assumed that Japan is currently in a transitional period. Discussions on this point should continue to be closely monitored.

6. The Impact of Emerging Technologies on the Security Environment in the Asia-Pacific Region

The *Defense of Japan 2021* White Paper[23] characterizes the Asia-Pacific region as follows.

> States in the Indo-Pacific region, including Japan, abound in political, economic, ethnic, and religious diversity. Also, each country has different security views and threats perceptions. Therefore, a regional cooperation framework in the security realm has not been sufficiently institutionalized, and longstanding issues of territorial rights and reunification in this region continue to remain.

These regional characteristics influence the scope, implementation method, and timing of applications of emerging technologies.[24] Therefore, with this in mind, I will discuss the impact on the security environment in the Asia-Pacific region for each of several representative fields of technology.

(a) EMS Technology

The EMS, along with space and cyberspace, is attracting attention as a new domain.[25] Whether the EMS should be treated as an independent domain like other domains is still open to debate.[26, 27] However, its nature of linking and supporting multiple domains is widely recognized.[28]

As suggested by various previous studies, EMS technology has the potential to increase our options in the gray zone and generate initiative to control situations.[29]

As an example, consider one application of EMS technology: directed energy weapons. With respect to effectors that produce some effect on a target, the only conventional means has been the projectile. Thus, although there are various types of projectiles, their use in the gray zone could not be an effective means because of the possibility of unintended escalation. On the other hand, directed energy weapons provide a third option that could not be realized with conventional projectiles: serving as effectors that influence a target through the transmission of energy by electromagnetic waves.

It is difficult for both the user of directed energy weapons and those they are used against to visually confirm the weapons' effects, which are conventionally possible to

confirm. Therefore, it is possible to intentionally use the weapons and then see the reaction of the other party. For this reason, no matter which country uses them, they can be expected to bring advantageous options for the side with the capability.[30]

On the other hand, considering the current situation in the region in which regional cooperation frameworks on security aspects are not sufficiently institutionalized, host-nation coordination (HNC)[31] for the use of radio waves is expected to pose significant difficulties. While this is not a problem that can be solved solely by technology, EMS management[31,32] is considered to become a major challenge in the application of EMS technology.

(b) Wide-Area Surveillance Including Space

In general, the enhancement of wide-area surveillance capabilities is essential for decision-making from the strategic to the tactical level.[33] The increasing use of space has expanded the scope of surveillance, which was previously limited by national borders, and has made it possible to check the surface conditions from above the country or region targeted for surveillance.

Against this background, technological challenges that are expected to be faced in future R&D include the realization of passive distributed detection supported by machine-to-machine communications[34] and advanced arithmetic processing, enhancement of the ability to equip sensors, as well as not only the miniaturization of sensors but also the use of open architectures[35] to ensure flexibility and rapid capability improvement.

Furthermore, in addition to the capabilities of the sensors themselves, sensor signal processing with limited power and sensor fusion algorithms for data from multiple signal sources are expected to be developed in order to efficiently process increasing amounts of data.

The impact on the strategic environment as a result of the development of these technologies is expected to be the need for deception and concealment premised on being the target of space-based surveillance in order to counter increasingly sophisticated surveillance capabilities. Thus, the technologies and methods to do so are expected to be further developed in the future.[36]

(c) Cyber Defense

Today, the stable use of cyberspace is the foundation for a wide range of defense activities. It goes without saying that the equipment system of systems is made up of networks. In order to support the operation of equipment systems, it is necessary to prepare for threats

not only from states but also from various non-state actors, and to ensure the use of cyberspace, which is essential for the operation of equipment.

The technical challenges for this include preventing damage to cyber systems incorporated in equipment and ensuring the operational continuity of systems necessary for defense.

The use of civilian technologies is indispensable to solve these technological challenges. However, the nature of the systems used for defense purposes makes it impossible to leave everything to the private sector. Therefore, the key will likely be for the defense acquisition community to always grasp threat trends, conduct outreach for the latest civilian technologies, and promptly apply those civilian technologies to individual pieces of equipment. This will require agile acquisition processes for rapidly acquiring capabilities that follow the business practices of the civilian sector, rather than the waterfall R&D processes often seen in traditional equipment R&D.[37]

(d) Unmanned and Autonomous Technology

With advances in autonomous technology, unmanned vehicles are expected to complement or partially replace the functions of traditional manned vehicles. In the Asia-Pacific region, the rate of population growth has slowed in recent years,[38] and some countries and regions are already in a stage of population decline like Japan. These countries and regions in particular are expected to benefit from unmanned vehicles.[30, 39]

To realize autonomous systems, in addition to acquiring technology to recognize the surrounding environment and integrating it into unmanned vehicles, it is necessary to consider command and control systems that include both unmanned and manned vehicles.

Japan, which is surrounded by water on all sides, can be expected to benefit particularly from the utilization of maritime drones.

(e) Hypersonic Technology

Unlike conventional ballistic and cruise missiles, hypersonic vehicles have the following characteristics:

1. Extremely short response times; and
2. Unpredictable flight paths.[40]

They are considered to be extremely difficult to intercept, and are cited as a representative example of a "game changer." Because it is impossible to distinguish the

type of warhead mounted based on the appearance of the projectile, it has been pointed out that hypersonic vehicles have the potential to undermine regional strategic stability.[40]

R&D for hypersonic vehicles is being advanced in Japan. Technological challenges include the establishment of heat-resistant technology to withstand aerodynamic heating at hypersonic speed and supersonic combustion technology. These technologies are considered to be still in the demonstration stage. In order to create equipment using these technologies, it is expected that they will be inexpensive enough to be procured as equipment commensurate with their expected effectiveness.

7. Quantitative Evaluation and Foresight Concerning Impact on the Security Environment Using Digital Technology

The various emerging technologies, including the ones I have explained above, undergo quantitative evaluation of their impacts that goes beyond qualitative discussions, and the key to foresight on their impacts is digital technology. Recent advances in computer hardware performance as well as in modeling and simulation technology have made it possible to perform complex engagement simulations that interweave several different types of units.[41] In the real world, these advances are increasingly enabling electronic warfare simulations using a broad EMS, which are difficult to carry out due to factors such as concerns about signal collection by potential adversaries as well as national and international regulations.[42] Such mission-level modeling and simulation technology can be used not only for training, but also as an opportunity to identify gaps in our own and the other's military capabilities and to consider means of filling them.[43] Digital technology can serve as a "bridge" between the R&D community and users. In the future, mission engineering is expected to bring a broader force-level perspective to the R&D community than the traditional systems engineering perspective. Furthermore, the following are expected to become possible through the use of digital technology:

1. Quantitative prediction of the impact of new technologies;
2. Support for the rationale on investment decisions in technology; and
3. Support for judgments on acquisition decisions.[44]

8. Conclusion

This report outlines the impact of investment in emerging technologies on the strategic environment in the Asia-Pacific region centered on Japan's perspective. In recent years, the private sector has become the main player in technology investment, but state investment in technology also continues to maintain a certain share, and investment in technology is seen as one of the tools of inter-state competition. As for the role of governments, they have been forced to optimize resources for future requirements while optimizing cost effectiveness.

To support the long-term perspective of stakeholders in R&D and procurement, the MOD has released two strategies that show the basic direction for its equipment policy and technology policy.

Because there is always uncertainty involved in predicting future warfare, scientists and engineers involved in defense need to be aware of strategic perspectives.

Given the characteristics of the Asia-Pacific region, the EMS, wide-area surveillance including space, cyber defense, unmanned and autonomous technologies, and hypersonic technologies have the potential to bring about irreversible changes in the regional security environment. Further use of digital technologies is expected for quantitative evaluation and foresight on the impact of these technologies, rather than being limited to qualitative discussions.

(All views expressed in this report are the author's own and do not represent the official position of the Acquisition, Technology & Logistics Agency or the Ministry of Defense.)

References

1 OECD, "Frascati Manual 2015", https://www.oecd-ilibrary.org/science-and-technology/frascati-manual-2015_9789264239012-en. Accessed 15 June 2022.

2 National Science Foundation, "Definitions of Research and Development: An Annotated Compilation of Official Sources", March 2018.

3 Jaruzelski, Barry, Robert Chwalik, and Brad Goehle. "What the top innovators get right." strategy+business 93 (2018).

4 OECD, "Main Science and Technology Indicators", September 2021.

5 Sechser, Todd S., Neil Narang, and Caitlin Talmadge. "Emerging technologies and strategic stability in peacetime, crisis, and war." Journal of Strategic Studies 42.6 (2019): 727-735.

6 Mazarr, Michael J., Jonathan S. Blake, Abigail Casey, Tim McDonald, Stephanie Pezard, and Michael Spirtas, Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2726.html.

7 Rotolo, Daniele, Diana Hicks, and Ben R. Martin. "What is an emerging technology?" Research Policy 44.10 (2015): 1827-1843.

8 Boon, Wouter, and Ellen Moors. "Exploring emerging technologies using metaphors: A study of orphan drugs and pharmacogenomics." Social Science & Medicine 66.9 (2008): 1915-1927.

9 Lichtenbaum, Peter, Victor Ban, and Lisa Ann Johnson. "Defining 'emerging technologies': Industry weighs in on potential new export controls." China Business Review 17 (2019): 2019.

10 Martin, Ben R. "Foresight in science and technology." Technology Analysis & Strategic Management 7.2 (1995): 139-168.

11 Adner, Ron, and Daniel A. Levinthal. "The emergence of emerging technologies." California Management Review 45.1 (2002): 50-66.

12 Sayler, Kelley M. Emerging Military Technologies: Background and Issues for Congress. Congressional Research Service Washington United States, 2020.

13 Department of Defense. "Department of Defense Dictionary of Military and Associated Terms." (2021).

14 Thaler, David E., Strategies to Tasks: A Framework for Linking Means and Ends. Santa Monica, CA: RAND Corporation, 1993. https://www.rand.org/pubs/monograph_reports/MR300.html.

15 Davis, Paul K. and Lou Finch, Defense Planning for the Post-Cold War Era: Giving Meaning to Flexibility, Adaptiveness, and Robustness of Capability. Santa Monica, CA: RAND Corporation, 1993. https://www.rand.org/pubs/monograph_reports/MR322.html. Also available in print form.

16 Troxell, John F. "Force Planning in an Era of Uncertainty: Two MRCs as a Force Sizing Framework." (1997).

17 Knopman, Debra, Don Snyder, Irv Blickstein, David E. Thaler, James A. Leftwich, Colby P. Steiner, Quentin E. Hodgson, Elaine Simmons, Krista Romita Grocholski, and Yvonne K. Crane, Proposed Analytical Products for the Air Force Warfighting Integration Capability: Developing and Presenting Options for Future Force Design and Capability Development. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR4199.html. Also available in print form.

18 Morgan, Forrest E. and Raphael S. Cohen, Military Trends and the Future of Warfare: The Changing Global Environment and Its Implications for the U.S. Air Force. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR2849z3.html. Also available in print form.

[19] Ministry of Defense, "Strategy on Defense Production and Technological Bases" June 2014, https://www.mod.go.jp/atla/soubiseisakuseisan.html. Accessed 25 March 2022.

[20] Ministry of Defense, "Defense Technology Strategy" August 2016, https://www.mod.go.jp/atla/en/policy/policy_strategy.html. Accessed 25 March 2022.

[21] "Research and development promotion policy, defense industry development policy and basic policy related to the production and development of equipment (notice)" July 16, 1970

[22] Brandt, Linda. "Defense Conversion and Dual-Use Technology: The Push Toward Civil-Military Integration." Policy Studies Journal 22.2 (1994): 359-370.

[23] Ministry of Defense, "Defense of Japan 2021" (2021).

[24] Sayler, Kelley M. Emerging Military Technologies: Background and Issues for Congress. Congressional Research Service Washington United States, 2020.

[25] "National Defense Program Guidelines for FY 2019 and beyond" (National Security Council decision, Cabinet decision) December 18, 2018.

[26] Sydney J. Freedberg Jr., "Spectrum (EW) Should Be A Warfighting Domain: Rep. Bacon", Breaking Defense, https://breakingdefense.com/2017/11/spectrum-ew-should-be-a-warfighting-domain-rep-bacon/. Accessed 25 March 2022.

[27] Garrett K. Hogan, "The Electromagnetic Spectrum: The Cross Domain", Joint Air Power Competence Centre, https://www.japcc.org/electromagnetic-spectrum-cross-domain/. Accessed 25 March 2022.

[28] CRS, "Defense Primer: Electronic Warfare", IF11118, Nov. 23, 2021.

[29] Clark, Bryan, Mark Gunzinger, and Jesse Sloman. Winning in the gray zone: using electromagnetic warfare to regain escalation dominance. Center for Strategic and Budgetary Assessments, 2017.

[30] Hornung, Jeffrey W., Scott Savitz, Jonathan Balk, Samantha McBirney, Liam McLane, and Victoria M. Smith, Preparing Japan's Multi-Domain Defense Force for the Future Battlespace Using Emerging Technologies. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/perspectives/PEA1157-1.html.

[31] Joint Publication 3-85, "Joint Electromagnetic Spectrum Operations (JEMSO)", May 2020.

[32] Department of Defense, "Electromagnetic Spectrum Superiority Strategy", October 2020.

[33] Alkire, Brien, Yool Kim, Matthew Berry, David Blancett, James Dimarogonas, Niraj Inamdar, Sherrill Lingel, Nicholas Martin, George Nacouzi, Joel B. Predd, and William A. Williams, Enhancing Assessments of Space Mission Assurance. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR2948.html. Also available in print form.

[34] Anton-Haro, Carles, and Mischa Dohler, eds. Machine-to-machine (M2M) communications: architecture, performance and applications. Elsevier, 2014.

[35] Collier, Charles Patrick, et al. "Sensor Open System Architecture (SOSA)." Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2016. Vol. 9849. SPIE, 2016.

[36] Vick, Alan J., Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR968.html. Also available in print form.

[37] DAU, "Adaptive Acquisition Framework", https://aaf.dau.edu/. Accessed 25 March 2022.

[38] United Nations, "World Population Prospects 2019", 2019, https://population.un.org/wpp/Publications/. Accessed 25 March 2022.

[39] Tate Nurkin and Ryo Hinata-Yamaguchi, "Emerging Technologies and the Future of US-Japan Defense Collaboration", Atlantic Council, April 2020.

[40] CRS, "Hypersonic Weapons: Background and Issues for Congress", March 2022.

[41] National Research Council. Modeling and simulation in manufacturing and defense acquisition: Pathways to success. National Academies Press, 2002.

[42] Adamy, David. Introduction to electronic warfare modeling and simulation. Artech House, 2003.

[43] Leftwich, James A., Debra Knopman, Jordan R. Fischbach, Michael J. D. Vermeer, Kristin Van Abel, and Nidhi Kalra, Air Force Capability Development Planning: Analytical Methods to Support Investment Decisions. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2931.html. Also available in print form.

[44] Department of Defense, "Mission Engineering Guide", Nov 2020.

Chapter 3
The Rise of the Chinese Techno-Security State and its Strategic Implications[1]

Tai Ming Cheung

The techno-security sphere is where economics, technological innovation, military power, and national security intersect and has become a principal arena for competition between established and rising great powers. China has become a central challenger to the United States for global techno-security dominance and this paper examines the components, characteristics, and development trends of the Chinese techno-security state.

The techno-security state refers to innovation-centered, security-maximizing regimes that prioritize the building of technological, defense, and national security capabilities to meet expansive national security requirements based on heightened threat perceptions and the powerful influence of domestic pro-security coalitions. A core premise behind the techno-security state concept is the pivotal role of the state in technology development, especially related to strategic and national security capabilities.

Four key dimensions of the Chinese techno-security state will be examined: 1) the centrality of national security; 2) the primacy of innovation; 3) the urgency of military transformation; and 4) the ambition of fusing the military and civilian spheres.

The Hard Turn of the Chinese National Security State

Upon taking office in 2012, Xi Jinping moved expeditiously to engineer a far-reaching reframing of the country's national security posture. There was no single seminal shock that triggered this hard national security turn. For China's realist-minded security policy makers at the helm in the early 2010s, the country's national security situation was complicated but manageable. The official assessment articulated by outgoing leader Hu Jintao in 2012 was that "the world today is undergoing profound and complex changes," but the overall "balance of international forces is developing in a direction favorable for the maintenance of world peace, creating more favorable conditions for overall stability

[1] This paper is derived in part from a longer book-length study of the Chinese techno-security state by the author that was published by Cornell University Press in 2022.

in the international environment."[2]

For Xi, however, these traditional realpolitik perspectives painted only a partial and far-too-rosy picture of China's actual security environment. He brought to office a very different set of assumptions and viewpoints as to what constituted the most worrying sources of dangers to the Party and the country and how they should be addressed. As a long-time provincial apparatchik, Xi's worldview was dominated by domestic and Party concerns. Xi was in particular haunted by the collapse of the Soviet Union that happened more than two decades ago.[3] Shortly after becoming paramount leader, in a speech asking why the Soviet Union and the Soviet Communist Party had collapsed, Xi said this was "a profound lesson for us. To dismiss the history of the Soviet Union and the Soviet Communist Party, to dismiss Lenin and Stalin, and to dismiss everything else is to engage in historic nihilism."[4]

Xi was determined that the Chinese Communist Party should avoid the same fate, even though China in the 2010s bore little resemblance to the late decrepit Soviet regime. Xi's answer was a hand-in-glove strategy of hard-hitting ideological purification and the building up of a repressive national security state. This need to prepare for danger in times of peace and to be ready for sudden incidents became important strands in the weaving of a tapestry that would eventually become known as the Holistic National Security Outlook (HNSO 总体国家安全观). Unveiled in April 2014, the HNSO has become the overarching conceptual framework for Xi's national security state. The country's first-ever national security strategy, which was issued in 2015, is derived largely from the HNSO.[5] A central argument of the HNSO is that "China now faces the most complicated internal and external factors in [its] history."[6]

At first glance, this statement would appear to be overly alarmist as China had endured existential nuclear threats from the U.S. in the 1950s and border clashes with

---

2 Hu Jintao, "Unswervingly Advance Along the Path of Chinese Characteristics, Struggle To Complete the Building of a Well-Off Society in an All-Round Way," Report to the Eighteenth Chinese Communist Party National Congress, 8 November 2012, *People's Daily*, 9 November 2012. http://politics.people.com.cn/n/2012/1109/c1001-19529890.html

3 See Evan Osnos, "How Xi Jinping Took Control of China," *The New Yorker*, 6 April 2015. https://www.newyorker.com/magazine/2015/04/06/born-red

4 "Leaked Speech Shows Xi Jinping's Opposition To Reform," *China Digital Times*, 27 January 2013. https://chinadigitaltimes.net/2013/01/leaked-speech-shows-xi-jinpings-opposition-to-reform/

5 "Xi Jinping Chairs Political Bureau Meeting on Outline for National Security Strategy," *Xinhua News Agency*, 23 January 2015. http://www.xinhuanet.com//politics/2015-01/23/c_1114112093.htm

6 "National Security Matter of Prime Importance: President Xi," *Xinhua News Agency*, 15 April 2014. http://www.xinhuanet.com//politics/2014-04/15/c_1110253910.htm

the Soviet Union in the late 1960s that nearly escalated into a full-scale war. But the point being made by the HNSO is that the dangers imperiling China in the twenty-first century are not the gravest that it has ever faced but the most complex. Based on Xi's reconceptualization of national security, the most dangerous threats are not external but internal, not traditional but non-traditional, not geo-strategic but political, and not in the here and now but emerging. From this vantage point, the world is a far darker and more menacing place, thus justifying the establishment of a strong national security state. So the concrete security environment that China faced in the early 2010s had not radically deteriorated, but the way its new leaders perceived the situation had been significantly altered.

On the issue of core national interests, the balance between development, security, and sovereignty has also been revised under Xi's tenure. From Deng Xiaoping to Hu Jintao, development was by far the most important national priority, but Xi has elevated security to the same level, if not higher. "We not only emphasize development issues but also security issues," Xi said at a meeting of the Central National Security Commission in April 2014.[7] Moreover, Xi said that national security and development are deeply intertwined with each other. "Security and development are two sides of the same issue, two wheels in the same driving mechanism. Security guarantees development, and development is the goal of security."[8] What this means is that China needs to pursue a more pro-active and assertive approach in shaping and protecting its security environment to promote development rather than its previously more reactive and low-key posture.

Innovation-Driven Development Strategy

The Innovation-Driven Development Strategy (IDDS 国家创新驱动发展战略) represents the Xi administration's bold overarching development strategy of realizing China's long-term ambition of becoming a world power by mid-century. The strategy is state directed but market supported, globally engaged but framed by techno-nationalist motivations. It seeks a seamless integration of the civilian and military domains, and employs a selective authoritarian mobilization approach targeted at core and emerging critical technologies.

---

7 "Xi Jinping Chairs First NSC Meeting, Stresses National Security with Chinese Characteristics," *Xinhua News Agency*, 15 April 2014. http://www.xinhuanet.com//politics/2014-04/15/c_1110253910.htm

8 "Xi Jinping's Speech at Opening of Second World Internet Conference," *Xinhua News Agency*, 16 December 2015. http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm

The Xi administration has set the implementation of the IDDS against a Hobbesian backdrop of a life-or-death struggle for the economic and strategic renaissance of China. Its leaders see the world as engaged in an intensive zero-sum technological revolution for national and military competitiveness that requires China to urgently get its innovation house in order so it can effectively compete for the global commanding heights. This assessment was made well before the sharp deterioration in U.S.-China relations in the mid- to late 2010s, which has only reinforced the Chinese leadership's belief that it has made the correct policy choices.

The IDDS represents a whole-of-nation effort in the pursuit of technological innovation. This allows the authorities access to enormous institutional capabilities and material resources that can be applied to critical objectives. This selective authoritarian mobilization model is what Xi calls the superiority of the socialist system and has been successfully used on a number of pivotal S&T projects in the past.

A key measure of the authoritativeness and ability of the IDDS to guide China's development is the extent and long-term commitment of top-level leadership support. The IDDS is personally intertwined with Xi, who first put forward the concept and was intimately involved in its formulation, approval, and rollout. In a political setting where power rests more in the person of Xi and less in institutions, the IDDS is likely to benefit from its tight association with Xi in at least two ways. First, Xi's strong commitment to the IDDS sends a clear signal to the administrative bureaucracy to vigorously implement the strategy and associated policies and plans or suffer the consequences. Second, the lifting of term limits in 2018 on Xi's tenure in power means that the IDDS can expect to enjoy an extended shelf life, which is important because of its long-term focus.

The IDDS framework also demonstrates the ambition and risk-taking appetite of the Xi administration in its goal of transforming China from a catch-up imitator into a world-class original innovator by the first half of the 2030s. This will require a fundamental overhaul of how the Chinese national innovation system has traditionally been organized, incentivized, and governed. The 14th Five Year Plan covering the 2021-2025 period provides the medium-term implementation roadmap for achieving this goal.

The IDDS has also promoted international S&T cooperation but selectively and on China's terms, of which ensuring that China has a prominent say in the making of the global innovation order is a top priority. Xi has said that it is essential for China to "plan and promote scientific and technological innovation with a global vision, comprehensively strengthen international scientific and technological innovation cooperation, actively

integrate into the global network of scientific and technological innovation, enhance the level of opening of up the state's science and technology programs to the outside world, actively participate in and lead international scientific projects, and encourage Chinese scientists to initiate and organize international scientific and technological cooperation projects."[9] One example of how China is developing its global innovation reach is through the Belt and Road Initiative, which Xi says should be used to build S&T innovation alliances, bases, and common platforms. Moreover, Xi says that it is important to enhance China's influence and rulemaking ability in global science and technology governance. This includes standards setting, norm making, and the building of international regimes and institutions, such as in cybersecurity and 5G.

The principal task of the IDDS and its constellation of associated plans and strategies is to support China's overall development, of which integral elements are national security and defense. While defense-related matters are only briefly touched upon in the IDDS, they are referred to throughout the outline that suggest that they are important but should not be drawn attention to. In the discussion on building a national innovation system, for example, there is mention of the need to "build a defense innovation platform for defense science and technology integration." When the outline states that China will contend for global innovation leadership by 2050, it also notes that "defense technology will have reached global leadership levels" by this time. Xi has sought to explicitly link the IDDS with the PLA's efforts to embrace innovation. At a meeting with PLA delegates at the annual National People's Congress in March 2016, Xi called on the PLA "to fully implement the innovation-driven development strategy, place combat capacity at the center of all their work, and step up theoretical and technological innovation."[10]

The indigenous development of strategic and core technologies is one of the foremost priorities of the IDDS and its associated plans and consequently receives plenty of attention. Strategic and core technologies refer to capabilities that are crucial for national security and long-term national competitiveness. The IDDS put forward a two-step development approach with the first near-to-medium stage to 2020 and the second long-term stage to 2030 (since extended to 2035). In the first step, the focus was on accelerating the implementation of megaprojects already underway with

---

9 "Xi Jinping Delivers a Speech at the Opening of the 19th Meeting of the Academicians of the Chinese Academy of Sciences and the 14th Meeting of the Academicians of the Chinese Academy of Engineering," *Xinhua News Agency*, 28 May 28 2018.

10 "Xi Jinping Attends Plenary Meeting of PLA Delegation, Stresses Comprehensive Implementation of Innovation-Driven Development Strategy and Promote Realization of New Strides in National Defense and Army Building," *Xinhua News Agency*, 13 March 2016.

the 2006-2020 Medium and Long-Term Science and Technology Development Plan (MLP). This includes high-end universal chips, basic software products such as operating systems, very-large-scale integrated circuit manufacturing equipment and turnkey techniques, new-generation broadband wireless mobile communication networks like 5G mobile communications capabilities, high-grade numerical control machinery and basic manufacturing equipment, large-scale advanced nuclear power plants with pressurized water reactors and high-temperature gas-cooled reactors, large-sized passenger aircraft, specifically the C919 airliner, high-resolution earth observation systems to allow the establishment of a comprehensive ground, atmospheric, and marine observation network, and manned spaceflight and lunar exploration projects like the Tiangong-2 space laboratory.

Military Strengthening

The possession of a strong, vibrant, and technologically advanced military and defense economic apparatus is pivotal to the forging of a potent techno-security state. Xi's thinking on the building of China's military power is formally known as "Military Strengthening in the New Era" (新时期的强军) and calls for a three-step transformation of Chinese military power to the middle of the twenty-first century.[11] The first step was to achieve the mechanization of the PLA by 2020 along with making major progress in the development of "informatization" and strategic capabilities. This has been largely accomplished. The second more ambitious phase is to "basically" complete defense modernization by 2035, which would mean that the PLA and the defense science, technology, and industrial base would have finally caught up with the world's top tier of advanced defense countries. The third and most challenging stage is for China to become a comprehensive world-leading military power by 2050, in which it would overtake the United States in global superiority.

One of the chief purposes of the Chinese techno-security state is to enable the development of a strong, technologically advanced, and politically reliable military establishment that is able to meet an expanding portfolio of missions and responsibilities. However, the PLA has rarely had the luxury of enjoying high-end military technological

---

[11] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," *19th Chinese Communist Party National Congress*, 18 October 2017, http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm.

self-reliance, which is a basic requirement for any aspiring great power. The development of strategic nuclear and ballistic missile deterrent capabilities in the 1960s and 1970s was one of those occasional moments when self-sufficiency was achieved in advanced military capabilities, but for the most part the conventional weapons system has struggled mightily because of chronic early dependence on imported Soviet technologies and know-how and deep-seated structural barriers that stymied coordination and development.[12]

There is rising optimism and expectation within the contemporary Chinese defense establishment that this dismal state of affairs is coming to a decisive end and the country will soon be able to join the world's advanced defense industrial powers at the global technological frontier. The overarching objective of Xi's military strengthening guidance is to catch up and lead as quickly as possible. This requires close coordination and collaboration between the military strengthening guidance, the IDDS, national security strategy, and military civil fusion (MCF) development strategy.

Xi began to put forward his ideas and thinking on military strengthening immediately upon becoming party general secretary and CMC chairman at the 18th Party Congress in November 2012. At an expanded CMC meeting following the congress, the new commander-in-chief instructed the assembled military chiefs that the PLA needed to step up its deterrent and combat readiness, be prepared for military struggle, and embrace a revolution in military affairs with Chinese characteristics.[13]

The application of Xi's high-level military thinking into the duties, missions, and responsibilities of the military establishment is the domain of the Military Strategic Guidelines (MSG), which is the Chinese version of a national military strategy and constitutes the PLA's "programs and principles for planning and guiding the overall situation of war in a given period," or how the PLA would prepare to fight a future war.[14] As the MSG is classified, any examination of its nature and contents is limited to circumstantial openly available information.

The Chinese government issued a 2015 defense white paper on "China's Military Strategy" that can be viewed as a circumscribed de facto public outline of the MSG

---

12 See Tai Ming Cheung, *Fortifying China* (Ithaca, N.Y.: Cornell University Press, 2009).

13 "Hu Jintao, Xi Jinping Attend Enlarged Meeting of Central Military Commission, Deliver Important Speeches," *Xinhua News Agency*, 17 November 2012.

14 Taylor Fravel, *Active Defense: China's Military Strategy Since 1949* (Princeton, N.J.: Princeton University Press, 2019), 28. See also David M. Finkelstein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,'" in Roy Kamphausen and Andrew Scobell (Eds), *Right Sizing the People's Liberation Army: Exploring the Contours of China's Military* (Carlisle, P.A.: Army War College, 2007), 67–140.

carefully edited to avoid disclosing any sensitive information. The white paper spelled out noteworthy adjustments to the country's military strategy, especially the need for heightened preparations for maritime conflict, information-era warfare, and the prioritization of the oceans, outer space, and cyberspace as the new "critical security domains."[15]

The white paper provided an assessment of the global strategic environment that highlighted several significant technological trends. The first was that the global revolution in military affairs was at a new stage and was "posing new and severe challenges to China's military security." A second feature of the rapidly evolving technological landscape was the emergence of new domains, of which outer space and cyberspace are emphasized as the "new commanding heights in strategic competition." A third accelerating trend was a fundamental change in the nature of warfare toward informationization, which refers to the information age and the rise of information-related processes and capabilities. The white paper pointed out that it was the "major powers" that are in the vanguard of this process and are "speeding up their military transformation and force restructuring."

The drafting of the 2014 MSG took place in the early years of the Xi administration and ahead of the completion of the major innovation, national security, and military strengthening strategies. All of these strategies point out that the 2010s was a transitionary stage of development and more deep-seated and transformative improvements will only materialize from the 2020s onwards.

Several of the key components of the 2014 MSG show signs of major change that cumulatively point to a consequential change to China's thinking and approach to future war. First is the concept of military struggle. From solely a war-fighting prism, the 2014 MSG made what appears to be a modest amendment from winning local wars under informatized conditions to winning informatized local wars. But some Chinese military analysts argue that the Xi regime introduced an important shift by broadening the scope of the meaning of military struggle to incorporate other dimensions of geostrategic struggle. PLA Senior Colonel Luo Derong pointed out that China should "combine military struggle with political and diplomatic struggle."[16] In addition, Luo points out that the 2014 MSG includes references to the HNSO that views China's national security

---

15 State Council Information Office, *China's Military Strategy*, 25 May 2015.

16 Luo Derong, "Action Guidelines for Armed Forces Building and Military Struggle Preparations: Several Points in Understanding the Military Strategic Guidelines in the New Era" (军队建设与军事斗争准备的行动纲领:对新形势下军事战略方针的几点认识), *China Military Science* (*中国军事科学*), no. 1 (2017), 88–96.

more expansively to cover economic and domestic affairs. Moreover, China has embraced the use of so-called grey zone tactics that blur the civilian-military divide.

Second is the identification of the strategic opponent. At the time that the 2014 MSG was being drawn up, the military-strategic competition between the United States and China was still in its infancy and the two countries continued to pursue cooperative working relations. From the mid-2010s, however, and especially with the arrival of the Trump administration in 2016, the pace, scale, and intensity of bilateral military rivalry escalated across the defense spectrum from defense technological competition to contested forward military deployments in the Asia-Pacific region and major adjustments in force structures directly targeting the other side.

The PLA had been very careful in its official public assessments of the United States as a military and strategic threat, but this began to change in the second half of the 2010s. While the 2015 Chinese defense white paper made only mild and indirect comments about the United States, the 2019 version is more pointed and direct in identifying the United States as the main culprit in undermining stability and challenging China's national security through "growing hegemonism, power politics, unilateralism, and constant regional conflicts and war."[17] The white paper adds that the United States "has provoked and intensified competition among major countries, significantly increased defense expenditures, pushed for additional capacity in nuclear, outer space, cyber, and missile defense, and undermined global strategic stability."

Military-Civil Fusion

At the heart of the Chinese techno-security state is the grandiose idea of a strategic economy that seamlessly serves civilian and military needs that Xi Jinping has vowed to create. In a keynote address at the 19th Party Congress in 2017, Xi called for the building of an "integrated national strategic system". This is a daunting challenge because of the long-standing and deeply entrenched separation between the civilian and defense sectors.

The means to achieve this integrated national strategic system is through military-civil fusion, which Xi has pursued since the mid-2010s. Before Xi took office, MCF (军民融合) was a mid-level policy priority that vied for attention with other issues. In 2015, Xi elevated MCF to a national-level priority and called this move a "major achievement

[17] *China's National Defense in the New Era* (Beijing: People's Republic of China State Council Information Office, 2019.

in our efforts of exploring the law of effecting well-balanced development of economic construction and national defense building over a long period and is a major policy decision based on the overall requirements of the national security and development strategies.'[18]

The rationale for a fundamentally different way of pursuing MCF compared with prior administrations was that the relationship between economic development and national security had significantly altered. The Xi regime now viewed military/security priorities as equally, if not more, important as economic priorities. The formulation of the MCF development strategy took more than five years to complete and steadily grew bolder and bigger over time. This can be largely attributed to Xi's increasing interest and involvement in MCF-related matters. At the beginning of his tenure, Xi was keenly interested and engaged in military modernization, national security, and science, technology, and innovation. As he intensively worked on these domains during his first several years in power, he came to appreciate the role that MCF would play as a crucial link between these topics. This learning experience led Xi to become more actively involved in MCF policy-making and strategic thinking from the mid-2010s onwards. This is most evident in Xi's appointment as the head of the Central Military-Civil Fusion Development Commission that was established in January 2017 to manage the MCF effort.

The MCF development strategy was formally approved in March 2018 and is officially known as the "Military-Civil Fusion Development Strategy Outline" (军民融合发展战略纲要). While this development strategy has not been publicly released, it is clear that MCF is a top priority for the Chinese civilian and military authorities.[19] The MCF development strategy represents a crucial link in Xi's efforts to coordinate between national security, economic development, and technological innovation. The strategy is the last piece in the jigsaw puzzle of national strategies that Xi has drawn up spanning from the IDDS to the HNSO.

---

[18] "Military-Civil Fusion Is the Strategic Decision for Enriching the Nation and Strengthening the Military," *Liberation Army Daily*, 17 March 2015.

[19] Jin Zhuanglong, "Opening Up a New Era for a New Situation for In-Depth Military-Civil Fusion Development," *Qiushi (求是),* 16 July 2018.

Conclusion

For the Chinese techno-security state, heightened threat perceptions, centralized top-down coordination and techno-nationalist dependence have been the principal drivers in its development. The Chinese authorities have used deepening concerns over the external security environment since the late 1990s, and especially the grand techno-security threat posed by the United States, as a catalyst to ramp up the development of its techno-security capabilities. This has especially been the case in areas such as strategic deterrence and anti-access/area-denial capabilities.

These perceptions of the U.S. threat have only grown more dire, pressing, and expansive under Xi's tenure and are a hugely powerful existential motivating factor in driving the long-term development of the Chinese techno-security state. Moreover, the aftermath of the Russia-Ukraine war can be expected to add to this impetus as the Chinese and Russian techno-security states enjoy a strong relationship of arms transfers and technological exchanges with each other that stretches back to the beginning of the 1990s.

Chapter 4
"Technological Innovation and Security": Japan's Innovation Strategy Based on Technological Patriotism

SUNAMI Atsushi

I. Techno-geopolitics and the new Cold War structure created by the United States and China: An economic security and innovation system
II. The system for developing advanced technology behind American and Chinese progress
III. The role of Japan and its "technological patriotism" in a new defense environment: Building an economic security innovation platform by securing "technological advantages"

Key Points

- China's rise in the domain of advanced science and technology and its race with the United States for global hegemony have sparked debates on economic security.
- China has both a system of implementing new ideas in society and the capability to expand into global markets by mass production—adequate qualities for becoming a technological hegemon.
- It is necessary for Japan to improve its technological innovation capabilities and create an economic system suited for the new security environment through cooperation between the public and private sectors via the economic security promotion bill.

"Economic security" has attracted attention both in Japan and abroad in recent years, and a concept similar to this in academic research is "economic statecraft," which was presented in the 1980s. However, the concept of economic security envisioned by Japan is even broader than that of economic statecraft. A bill for promoting economic security currently under Diet (Japanese parliament) deliberation has also been discussed within the "Advisory Panel on Economic Security Legislation" chaired by Professor Aoki Setsuko of Keio University, of which I am a member. Our discussion covered a broad range of issues, with particular emphasis on the four pillars of "building robust supply

chains," "securing core infrastructure," "developing advanced technologies through cooperation between the public and private sectors," and a "system of non-disclosure of patent applications."

Approaches to Economic Security

Debates on economic security are informed by various studies. Among these are studies focused on international politics, where issues in "arms control" such as arms export control and nuclear non-proliferation in particular are examined through the lenses of international relations. Also relevant are political science studies on new domains such as space and cyberspace.

Next, there are studies on major companies and small and medium-sized enterprises involved in basic defense-related industries as subjects of industrial analysis in Japan mainly from the viewpoint of economics, although not many of such studies exist. With the establishment of the Acquisition, Technology & Logistics Agency (ATLA) in 2015, there is an emerging need for company-specific investigations into what technology exists in particular areas of Japan.

The current economic security policy started from a proposal made by the Liberal Democratic Party's "Strategic Headquarters on the Creation of a New International Order" (later renamed the Headquarters for Economic Security Measures, Policy Research Council) in December 2020. The proposal presented the perspectives of "strategic autonomy" and "strategic indispensability," whose establishment requires Japan to take the initiative in shaping international rules. In addition, the proposal also pointed to the importance of security clearance (SC), through which the eligibility of personnel who handle confidential information is assessed. Currently, there are quite a few voices calling for a cautious approach to the introduction of SC, but the debate is expected to continue.

A basic idea behind technological innovation is that openness and diversity are the cornerstones of science, and that it is important to secure an environment where original ideas can be disseminated and researchers around the world can compete and collaborate in their research. At the same time, the coexistence of economic security with the freedom of economic activity is also an important issue in the course of promoting the former. It is necessary for policies to be implemented based on the balance between security and economic activity—concepts that may conflict with each other in some cases. The Keidanren (Japan Business Federation) has also made recommendations while

taking a strong interest in the issue, and it is essential to have close discussions with private companies in this regard.

China's Rise through its Advanced Technology

The handling of "dual-use" technologies for both civilian and military purposes is also a difficult issue. Since the Sputnik crisis in 1957, the United States has promoted security innovation while utilizing dual-use technologies. In the midst of this, China's rise is undoubtedly one of the significant factors that have triggered the debate on economic security, and how Japan balances its relations with China, which continues to pursue economic development, with its own security considerations has become an equally important issue.

Recently, it has been said that a "new Cold War structure created by the United States and China" has emerged in geopolitics, but the current US–China relations are totally different from the past Cold War era between the United States and the Soviet Union because the United States and China have close economic ties that are mutually complementary. Having said that, many Americans feel a strong sense of crisis when confronted with China's aspirations to become a hegemonic power in the world.

The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000 by Paul Kennedy was a bestseller back in the 1980s, which led to a sensational debate over the plausible hypothesis that the era of the United States had ended and the question of whether Japan could become the next hegemonic power. The wariness of Japan among American researchers subsequently faded away, however. Currently, *Destined for War: Can America and China Escape Thucydides's Trap?* by Professor Graham Allison of Harvard University has been selling well, which makes me feel that the times have changed dramatically over the past forty years.

What we should keep in mind when thinking about China is the concept of techno-hegemony. It has been pointed out in the United States that techno-hegemony consists of two factors: (1) universities with technological development capabilities and a system of industry-academia collaboration to introduce them to society; and (2) mass production capabilities. A country with these two elements can become the technological hegemon of its era. The United Kingdom after the Industrial Revolution, Germany when it challenged the United Kingdom, the United States during the postwar era, and Japan when it challenged the United States in the late 20th century can be considered to have been in this category.

In my view, China meets these two requirements. China's Peking University and Tsinghua University have world-class technological prowess, and China has had very active industry-academia collaboration for a long time. In addition, China has a mass production system because its collaboration with developed countries, including Japan, has enabled the factory construction projects in China to be accelerated. Ironically, Elon Musk, CEO of Tesla, Inc., had chosen China as the company's mass production base for its electric vehicles. China announced its vision of "Made in China 2025" in 2015, which should be taken seriously as China's pursuit of technological hegemony.

Russia, which is attracting renewed attention for its invasion of Ukraine, is unlikely to become a technological hegemon like China. It is true that Russia has great technological capabilities in cutting-edge fields such as space, medicine, and nuclear power. However, Russia lacks mass production capabilities. This is likely because Russia enjoys abundant natural resources, including oil and natural gas, and it has not invested much in that area.

The concept of "techno-geopolitics" is also attracting attention against the backdrop of the techno-hegemony that China is seeking to achieve. This means that countries are dynamically expanding into areas where no hegemony has been established, such as space, cyberspace, and even the Arctic Circle.

The Effects of Economic Sanctions on Russia

One concept that has been gaining attention in the context of economic security is that of "economic statecraft." This concept means that a country exerts its influence over other countries via economic means rather than military means to achieve its geopolitical national interests. This concept was first coined in academia by the international political scientist David Baldwin, who had taught in the 1980s at Columbia University, where I studied. He argued that it has become very effective and important for the state to use not only military means but also economic means to achieve its strategic goals. After the publication of his book, I also attended one of Professor Baldwin's lectures, in which he said, "This is a concept that is difficult to demonstrate empirically. There have been no successful cases." It is indeed difficult to point to actual cases in which a country has succeeded in altering the actions of other countries and achieved its strategic national goals via economic means alone. It is not surprising that such a concept exists, however.

The current economic sanctions imposed on Russia in response to its invasion of Ukraine is a form of economic statecraft. Imposing sanctions in a coordinated manner can send the message that the international community collectively disapproves of

Russia's actions. This signaling is effective to some extent. However, if some countries oppose the sanctions, it will instead expose the fact that international public opinion is divided, which could backfire.

Furthermore, because there is usually a powerful backlash from countries targeted by sanctions, it is necessary to consider in advance the second and third rounds of economic sanctions following the first. However, such prolonged sanctions may not ultimately lead to a settlement. This possibility is a cause for concern in the case of Russia as well.

"Principles" That Are More Important Than the Four Pillars

The economic security bill that the government is currently working on consists of four pillars: (1) securing supply chains for important supplies; (2) a preliminary review of core infrastructure facilities; (3) promoting the development of advanced technologies; and (4) the non-disclosure of patents.

These four pillars are important because they serve as the starting point of economic security. I believe the first part of the bill describes the significance of these pillars by outlining the basic ideas that undergird them. In other words, the legislation suggests that under the current state of international affairs, every economic activity is not solely governed by economic logic but instead approached with security or national survival as the primary goal, which makes economic activities also subject to intervention by state power. While there were some cautious voices within both the ruling and opposition parties, this idea was eventually incorporated into the bill.

The key issues to be addressed in this context are the establishment of penalties and the introduction of SC as mentioned above. These are essential rules if Japan were to participate in the Five Eyes alliance, where English-speaking countries, including the United Kingdom and the United States, share classified intelligence.

It is also critical for Japan to secure "technological advantages" based on these foundations. The rest of the world will take no notice of Japan in the first place if it does not have technologies that other countries crave, such as "made-in-Japan semiconductors," "made-in-Japan space technology," and "made-in-Japan vaccines." How we can strengthen innovation, which is the key to all this, is also inextricable from security. It is necessary for us to take urgent and effective action suited to Japan's circumstances to build a "dual-use innovation ecosystem." We are now in an era when policy interventions are essential for every economic activity, including research and development. I sincerely hope that the Japanese public will gain a deeper understanding of this issue through the current debate

on the economic security bill.

*Editor's note: This manuscript was received on April 18, 2022, prior to the enactment of the Economic Security Promotion Act on May 11, 2022.

Chapter 5
Technological Change and Future Security in the Indo-Pacific: An Australian Perspective

Malcolm Davis

Introduction

In 2020, the launch of Australia's Defence Strategic Update, and its accompanying Force Structure Plan, on 1st July 2020 by Prime Minister Scott Morrison, set the basis for future development of Australian defence policy and military strategy, and the future force structure of Australian Defence Force (ADF) in coming decades.[1] Both documents highlighted the importance for new types of military capability for the ADF, ranging from enhanced long-range strike through to sovereign space capability and investment in autonomous systems.

More recently, the signing of the 'AUKUS' agreement on 16th September 2021 opens new opportunities for Australia to invest in new types of critical and emerging technologies that could transform our approach to military operations in the Indo-Pacific and allow us to undertake a paradigm shift in our approach to military affairs.[2] Certainly, the most prominent aspect of AUKUS was the decision by Australia to acquire nuclear powered (but not nuclear-armed) submarines. However, an arguably more important and immediate outcome will be cooperation in areas such as artificial intelligence (AI), quantum technology, autonomous systems, hypersonics, cyber and space capabilities.

These and other areas of critical and emerging technologies will have a decisive impact on not only the character and conduct of future warfare but will likely reshape the geopolitical and military dynamics of the Indo-Pacific. The significance of embracing rapid innovation and change in military affairs, highlighted by both the 2020 Defence Strategic Update and then the 2021 AUKUS agreement has been reinforced by two further key developments – the 2021 AUSMIN summit in Washington DC, and then the Quad summit. The AUSMIN summit was important in expanding force posture arrangements in terms of allowing greater access for US forces to Australian facilities and territory and expanding cooperation in areas such as space and cyber.[3] The historic Quad summit expanded our links with Japan and India in areas of critical and emerging technologies that have military application, and expanded our cooperation with key

partners in key areas such as space, maritime domain awareness, and cyber security, amongst other areas of cooperation.[4]

These important developments in Australia's geopolitical role are not occurring in a strategic vacuum. They are occurring against a strategic context of intensifying strategic competition between a rising authoritarian China and the United States, and its key allies, including Japan and Australia. In terms of military capabilities that will decide this competition, the answer may very well not be traditional 'legacy' systems such as warships, aircraft, or ground forces – though those will remain highly important – but advantage in new domains, such as space and cyberspace, and with critical and emerging technologies.

This paper seeks to explore how these new types of military capability will play a role in this more dangerous strategic future, using current Australian defence policy as a starting point, and exploring likely next steps in terms of ADF capability development and force posture.

Technological change and Australia's strategic context

Australia faces a more precarious and unpredictable strategic environment in 2021 than perhaps at any time since the conclusion of the Second World War in 1945. The rise of an assertive People's Republic of China which is challenging security across a free and open Indo-Pacific, whilst rapidly modernising and expanding its military, is resulting in intensifying strategic competition between Beijing and Washington DC.[5] China seeks to challenge US strategic primacy in the region, in a manner that would be catastrophic for US interests. Likening current US-China competition to the ancient game of 'go', Rory Medcalf notes that

> "Over the past decade, the Chinese leadership has chosen to confront Japan in the East China Sea, Vietnam and the Philippines in the South China Sea, India on the disputed border and United States across the global board, from the western Pacific to cyberspace…" and argues that
> "Alone among the great powers, China's Indo-Pacific strategy connects directly with the survival of the domestic political system and the vested interests of the leadership."[6]

In other words, for the Chinese Communist Party (CCP) leadership, and especially

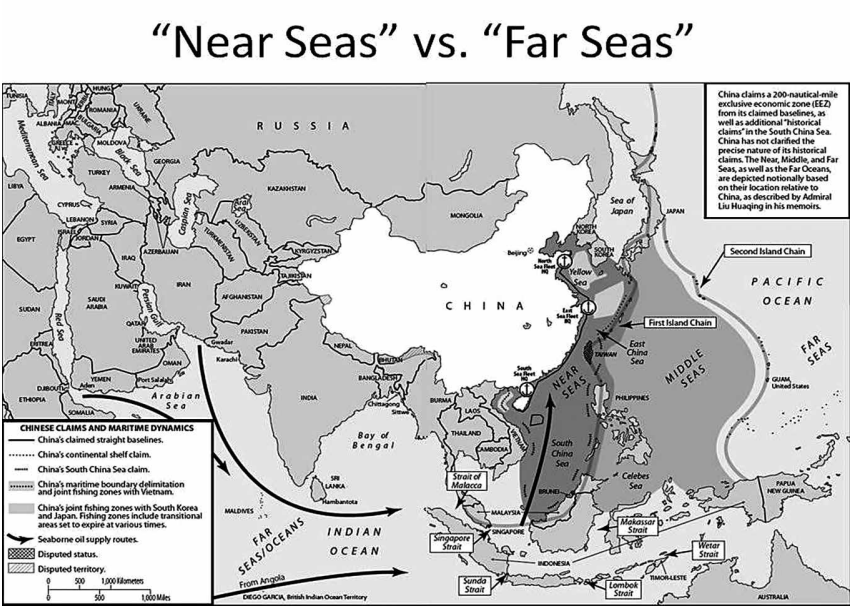
for President Xi Jinping, their legitimacy and grip on power depends on achieving the 'China Dream' of a rejuvenated China that is a rich country with a strong army. Success and continued political legitimacy demand that China resolves territorial disputes in a manner that overturns a perceived 'century of humiliation' lasting from the beginning of the Opium Wars in the 19th century through to the end of the Second World War and China's civil war in the mid-20th Century. Resolving these territorial disputes – the unification of China and Taiwan, China's claims to disputed territories and maritime zones in the South China Sea encircled by a Chinese drawn 'nine-dash line', and China's claims to the Senkaku islands in the East China Sea – are essential if the 'China Dream' is to be achieved by 2049, the centennial of the formation of the People's Republic of China.[7] China also has territorial disputes with neighbouring India in the Himalayas, which has recently generated increasing tension and even skirmishes between Chinese and Indian forces.

More broadly, China's rapid modernisation and expansion of the People's Liberation Army (PLA) is upending strategic dynamics that have traditionally favoured US power.* The growth of Chinese military power is occurring broadly in two trajectories. Firstly, the development of a counter intervention capability based around highly capable and increasingly long-range anti-access and area denial (A2AD) systems that will allow China to effectively raise the cost of US military intervention into the western pacific in a crisis to unacceptable levels, and strike at forward deployed US forces within the first and second island chains.[8] Secondly, China is building power projection capabilities, based around the world's largest Navy, together with Chinese Coast Guard and maritime militia vessels. The objective is to protect Chinese interests, including its diaspora and to ensure access to key resources in far flung deployments well beyond the first island chain (see map 1).[9]

China's Belt and Road Initiative (BRI), and notably, the 21st Century Maritime Silk Road, aligns neatly with these key interests from the South China Sea into the Indian Ocean, to access vital energy resources from the Persian Gulf, and through the Red Sea and Suez Canal into the Mediterranean Sea to markets in Europe.[10] The establishment of Chinese bases in Djibouti and more recently in Cambodia, and an attempt to establish a base in the UAE, is matched by dual-use commercial ports and airports, constructed under the BRI that ultimately, will support PLA power projection to the far seas and far oceans.[11]

---

* The People's Liberation Army includes not only the ground forces, but also PLA Navy (PLAN), PLA Air Force (PLAAF), PLA Rocket Forces (PLARF), PLA Strategic Support Force (PLASSF), PLA Joint Logistics Support Force, and People's Armed Police



Source: Andrew S. Erickson, Abraham M. Denmark, Gabriel Collins, "Beijing's 'Starter carrier' and Future Steps: Alternatives and Implications", *Naval War College Review*, 65.1 (Winter 2012), p. 22-23.

At the same time as China is expanding its military power and physical presence, it is promoting an alternative model of governance and development that challenges the dominance of western liberal democracy. This, in effect, amounts to an ideological challenge to western interests and Chinese actions would challenge the assumption by many western commentators and academics that the current growing tensions between China and the United States are not indicative of a new Cold War. H.R. McMaster notes that

> "China has become a threat because its leaders are promoting a closed, authoritarian model as an alternative to democratic governance and free-market economics. The Chinese Communist Party is not only strengthening an internal system that stifles human freedom and extends its authoritarian control; it is also exporting that model and leading the development new rules and a new international order that would make the world less free and less safe."[12]

Key regional US allies, including Japan and Australia, are responding to this comprehensive global challenge, and the growing risk of major power war emerging from these potential flashpoints by shifting defence policy in major new directions. The previous close focus on global counterterrorism has been replaced by a greater priority towards countering major power threats from China, as well as Russia. In particular, the possibility of a crisis emerging across the Taiwan Straits within this decade is now concentrating the minds of defence planners and strategic thinkers in Washington, Canberra, and Tokyo, as well as other capitals.[13] In Australia there is an increasingly active debate on the prospect for a cross-straits conflict, and how Australia should respond in the event that the United States, in choosing to support Taiwan in the face of a Chinese attack, calls on Canberra to assist its operations.[14]

With this deteriorating security outlook in mind, it is therefore no surprise that Australia's 2020 Defence Strategic Update (DSU), and its accompanying Force Structure Plan (FSP), released on 1st July 2020, alluded to a more contested and dangerous strategic outlook. The DSU highlights growing risks of major power war, potentially between China and the United States, noting that

> "Strategic competition, primarily between the United States and China, will be the principal driver of strategic dynamics in our region."[15]

and continues to state that

> "Major power competition, coercion and military modernisation are increasing the potential for and consequences of miscalculation. While still unlikely, the prospect of high intensity military conflict in the Indo-Pacific is less remote than at the time of the 2016 Defence White Paper, including high-intensity military conflict between the United States and China."[16]

The 2020 DSU also withdrew the traditional assumption of a period of ten years of strategic warning time, which has been a central feature of Australian defence policy since the late 1980s, stating that

> "Previous Defence planning has assumed a ten-year strategic warning time for a major conventional attack against Australia. This is no longer an appropriate basis for defence planning."[17]

The DSU highlights the challenges of growing coercion, competition, and grey-zone activities by China, directed against Australia and growing military capabilities appearing in the region that undermine the credibility of a ten-year period of warning time. The DSU also notes accelerating military modernisation driven by long-periods of economic growth, which is now undermining Australia's traditional military-technological advantages. It points to the introduction of "…advanced strike, maritime surveillance, and anti-access and area denial technologies, which have implications for Australian operations in the region."[18]

Finally, the DSU highlights emerging and disruptive technologies, including "… sophisticated sensors, autonomous systems and long range and high-speed weapons", as well as expanding cyber capabilities.[19]

With these trends clearly emerging, Australia is moving to invest in a range of new types of military-technological capabilities to meet the challenge posed by China's growing military power. Perhaps most significantly are investment in new long-range strike capabilities, initially alluded to in the 2020 Force Structure Plan (FSP), and then 're-announced' in the AUKUS agreement. Also of key importance were agreements to collaborate in new types of military technology areas, with AUKUS stating that areas to be considered initially would include "…cyber capabilities, artificial intelligence, quantum technologies, and additional undersea capabilities."[20]

The 2020 FSP also reinforces these priority areas, and in addition highlights the growing importance of space as an operational domain, noting that 'Space Control' is now a key task for Defence.[21] The elevation of the Space Domain, and the importance given to acquiring sovereign space capability, is a key step in opening up a broad range of new types of military capabilities for the ADF, including long-range strike, sovereign controlled space-based intelligence, surveillance and reconnaissance (ISR) and positioning, navigation and timing (PNT), and advanced logistics. The decision by Defence to establish a Defence Space Command as of 2022 reinforces this important step towards a more sophisticated approach to space operations.[22]

These recent developments in Australian strategic policy highlight a recognition of the importance of critical and emerging military technologies, and new operational domains in future warfare. Although the nature of war hasn't changed from its Clausewitzian fundamentals, the character and conduct of military operations are being transformed as new technologies, in particular, those emerging from civil and commercial sectors, are being adapted for military roles. Traditional air, naval and land forces remain of key importance, but the changing strategic environment, and the acceleration of technological

innovation as well as the importance of space and cyberspace as operational domains, are driving the embrace of new types of capabilities.

For Australia, there are risks and opportunities inherent in new domains and emergent technologies. A clear risk that is generating growing debate within Australia's strategic policy community is the growing disconnect between the clear dangers inherent in a rapidly worsening strategic outlook against the slow pace of military capability acquisition managed within Australia's defence organisation.

Recent steps such as AUKUS and the 2020 Defence Strategic Update suggest that Australian decision-makers are clearly ready to invest in emerging technologies. However, this is constrained by investment in major capability projects, for example, the Navy's *Hunter* class future frigates and the decision to acquire nuclear powered submarines under AUKUS.[23] A decision to proceed with substantial investment into new armoured fighting vehicles (AFVs) for Army under defence project LAND-400 Phase 3, continues to reinforce a more traditional approach to capability acquisition that is ill-suited to a more unpredictable strategic environment, and does not consider the practical aspect of how large and heavy AFVs can contribute to tactical or operational success in what is likely to be primarily an air, sea, space and cyber war in any probable future contingency involving China.[24] This approach to acquisition is slow, measured over project cycles of decades, and often emphasises a 'like for like' replacement mindset of incremental improvement that replaces older capability with similar numbers of more modern but similar platforms, rather than explore entirely new force structures better appropriate to radically different operational environments. Such an approach will be quickly outpaced by both events in a rapidly evolving region, and by the accelerating pace of technological change. The risk of project delays and cost overruns further raises the risk of capability gaps emerging.

Furthermore, the emphasis in current ADF force planning remains on small numbers of very expensive, 'boutique' capabilities which reinforce a brittle force in terms of combat sustainability in a high-intensity interstate or major power war contingency. Such an approach to ADF force structure, very appropriate for past strategic environments that was largely absent of a major power threat, and which enjoyed a ten-year strategic warning time, is no longer necessarily 'fit for purpose' in the future challenges facing Australia.

Clearly, it is time to challenge outdated paradigms for capability development, and a key step must be for the Australian defence organisation to be willing to accept change. Now is the time for such a shift in mindset, which can only be led from the top-down

at the direction of government, whilst new ideas on how best to shape the future ADF take hold. Australia *can* exploit new opportunities in investing in emerging technologies and building capabilities for new operational domains including space and cyberspace. AUKUS, and the 2020 DSU and FSP, together with collaboration with other partners, such as Japan and India through the Quad, open new pathways for Australia to take different approaches to building the future force, and ideally, accelerate the acquisition of advanced military capabilities more suitable to meeting the challenges on the horizon. It is vital for Australia that it rapidly moves to respond to a more demanding strategic context with new types of military capability, and shape ADF military strategy to best respond to a new era in Australian defence policy.

Key themes in the technology of future war

The most important force structure decision emerging from the 2020 Defence Strategic Update and the Force Structure Plan was a recognition that Australia needed advanced long-range strike capabilities in the face of growing Chinese military power, including, the development of Chinese long-range ballistic and cruise missiles armed with conventional warheads. The upgrade to Australia's long-range strike capabilities will initially be based around current missile systems such as the AGM-158C Long-range antiship missile (LRASM), of which up to 200 will be acquired, together with other systems such as Joint Air to Surface Attack Missile Extended Range (JASSM-ER) and the Tomahawk Land-attack Missile (TLAM).[25] However, the FSP also highlighted growing investment into much more capable hypersonic weapons for future acquisition. The AUKUS agreement reinforced the importance of long-range strike in the ADF.[26] Finally, the decision to establish local manufacturing of advanced missile systems gives Australia the ability to address challenges associated with combat sustainability in the face of high intensity major power war, especially if that war is protracted in nature.[27] It seems unlikely that global supply chains for such missiles would be sustainable in such a scenario, demanding sovereign missile production.

The acquisition of these new strike capabilities, and the decision to proceed with sovereign missile manufacturing, marked the end of a traditional mindset that largely saw the ADF undertake a 'defence in depth' approach to 'Defence of Australia' task from behind or inside the 'sea-air gap' to Australia's north and west, relying heavily on the United States for direct military assistance. Instead, Australia would seek to achieve greater self-reliance and project military force well forward of that notional strategic

'moat', which no longer provided any degree of operational and tactical protection against a range of emerging missile and non-kinetic threats. Chinese long-range anti-access and area denial capabilities meant that Australia had to defend its territory deep into the Indo-Pacific region. It's growing cyber, counter-space and electronic attack capabilities add to the risk posed by a positional defensive posture that is limited in reach and purely defensive in nature. The transition towards hemispheric operations could be seen to be a shift towards a form of 'forward defence in depth.' [28]

But to make such a strategy viable, the Defence organisation and the ADF now need to consider acquiring a panoply of emerging military technologies that could reshape the ADF to ensure it remains operationally relevant and fit for purpose in future war. Some broad themes of future war can be summarised as follows, which should guide future ADF capability development, and thus, shape Australia's ability to 'shape, deter and respond' across the Indo-Pacific region. [29]

Accelerating tempo of operations

Future warfare is likely to occur at a much faster pace, in terms of the generation of precision kinetic and non-kinetic effects over long range, and in terms of battlespace command and control. The impact of varying degrees of automation and high speed in military systems of systems will exceed the ability of human decision-makers, including political leaders, to manage. This will increasingly demand greater investment by Australia in artificial intelligence (AI) and there is a requirement to move more rapidly towards enabling varying degrees of autonomy across a complex, multi-domain operations environment.

The speed and pace of future military operations in a complex multi-domain battlespace is likely to occur over very long range, particularly in the Indo-Pacific region. The growth of China's long-range missile capabilities will challenge the ability of US and allied air and naval forces to project presence into maritime east Asia, or to survive within a highly contested A2AD envelope. However, for those missile systems to be effective, China must have a resilient ocean surveillance capability via satellites, high altitude drones, and ground based sensors. This network between the 'sensor and shooter' is the vital enabler for China's A2AD capabilities.

With that in mind, a requirement for resilient sensor to shooter links will accentuate the importance of gaining and maintaining a speed advantage, in addition to gaining and sustaining a knowledge edge. In the 1991 Persian Gulf War, the multi-national coalition

quickly gained a decisive advantage over Iraq because it had an assured knowledge edge that allowed it to operate well inside the decision cycle – the 'OODA loop' – of the Iraqi military.[30]

In future war, it is not at all certain that US and allied forces would be able to quickly gain and maintain such a knowledge edge, and a protracted, but rapid struggle for digital dominance is likely to emerge. This could initially take the form of a new 'battle for the first salvo' involving decisive military strikes within the space and cyber space domains, and across the electro-magnetic spectrum, as a prelude to or concurrent to military operations in traditional domains of air, sea, and land. This implies the possibility of a modern cult of the offensive, as the side which strikes most decisively and most rapidly, leaves their opponent effectively deaf, dumb, and blind, and unable to regain the battlespace initiative. The loser must then struggle to regain and reconstitute lost capability in space, counter ensuing cyber-offensives and defeat adversary electromagnetic operations. An inability to restore vital C4ISR networks would leave traditional air, sea and naval forces severely degraded in effectiveness, particularly in the face of new threats such as hypersonic weapons.

Autonomous Weapons and swarming

The ADF are moving ahead with experimentation in autonomous systems across all traditional domains of land, sea and air, and are investing in some key capabilities. For example, the Royal Australian Air Force (RAAF) is acquiring the MQ-4C Triton high altitude long-endurance UAV to partner with crewed P-8A Poseidon maritime patrol and response aircraft, as well as the MQ-9B Sky Guardian armed remotely piloted UAV. [31] Defence is also supporting local development of the Loyal Wingman Airpower Teaming System that will provide crewed-autonomous teaming capabilities for armed UAVs alongside crewed combat and combat support platforms such as the F/A-18F, F-35A and E-7A Wedgetail.[32] Australia's Defence Science and Technology (DST) group host regular autonomous technology experimentation events, such as 'Autonomous Warrior' and the 2022 Maritime RobotX Challenge.[33]

With these systems, humans are currently 'in the loop' and have direct control over lethal military systems. Current trends in autonomous systems suggest a transition to being 'on the loop' by giving greater degrees of trusted autonomy to a range of uninhabited and autonomous military systems in the air, at sea on or below the waves, and on land. The constraints of ethical, moral, and legal practices, including Jus in Bello

and international humanitarian law weigh heavily on the minds of military planners considering the application of these capabilities, at least in western liberal democracies. [34] However, it may be the case that adversaries choose to move faster in this transition and are even prepared to go further, potentially considering the benefits of humans fully 'off the loop' through fielding fully autonomous military systems that are directly controlled by AI. The moral, ethical, and legal dilemmas that are so constraining for governments in western liberal democracies may not be as acute for authoritarian states that are answerable only to themselves.

Australia's approach to autonomous systems is highlighted in several concept papers and strategy documents. For example, the Royal Australian Navy's 'Remote Autonomous Systems – Artificial Intelligence 2040' (RAS-AI 2040) strategy explains the RAN's perspective on the introduction of autonomous systems in coming decades.[35] It considers likely technology development in terms of autonomy, interoperability and communications, and secure computing and networking, and then explores the likely maritime missions that could be accomplished now, the potential tasks in the near term out to 2030, and then the possibilities for the far term by 2040.

Similarly, the Royal Australian Air Force 'HACSTRAT' paper seeks to rapidly deliver a path to future air and space capability that is integrated into the joint force. It notes that

> "The force of tomorrow will be characterised by invisible connections across air, land maritime, space information and cyber – with masses of data from sensor inputs fused with artificial intelligence and machine learning – to rapidly convert data to information to knowledge and to insight at unfathomable speeds."[36]

Like Navy's RAS-AI 2040, Air Force's 'HACSTRAT' emphasizes the role of AI to enable autonomous systems to augment crewed aircraft and human activity. It notes that crewed platforms will be force multiplied using robotic and autonomous systems, which enable increased mass, and exploit miniaturisation. It suggests a growing preponderance of 'remotely or autonomously piloted' systems as well as the use of hypersonics to 'help us reach further faster', and notes that 'space will become increasingly pivotal.'[37] Most importantly, HACSTRAT challenges traditional approaches to capability design in a way that is deliberately disruptive and designed to 'jolt Air Force out of its comfort zone.' As quoted in the HACSTRAT document, Air Commodore Philip Gordon, former DG Air and Space, states "…if we 'status quo' our way to the future we will fail."[38]

The Australian Army too has an approach to robotic and autonomous systems,

outlined in its 2018 Robotic and Autonomous Systems Strategy, and more recently within the 2020 Joint Concept for Robotic and Autonomous Systems.[39] The latter document highlights that robotic and autonomous systems

> "…provides Defence the opportunity to achieve greater combat power within its planned budget by increasing its physical and non-physical mass. It challenges an assumption that Australia cannot achieve mass compared to regional competitors as RAS offer the potential for Defence to increase the scale of effect that can be employed within planned resources."[40]

This is a key feature associated with development of advanced autonomous systems, that are either controlled directly by an AI on board an uninhabited platform, or from a command-and-control network incorporating AI. The possibility of a return of mass to the battlespace, in which 'quantity has a quality of its own' represents an important shift away from reliance on ever smaller numbers of ever more complex and expensive crewed systems, in the air, at sea and on land. Swarming in warfare, involving large numbers of loitering munitions, and low-cost armed drones suggests a future warfare scenario in which these systems attack legacy platforms in large numbers, overwhelming their defensive systems, and challenging their continued relevance and efficacy. This has already been glimpsed in the recent conflict between Azerbaijan and Armenia in 2020, in which Azerbaijan employed large numbers of drones to devastate Armenian ground forces.[41] In future war it is likely that swarming as a tactic, employing low cost 'kamikaze drones' and 'loitering munitions' of the sort employed in the Azerbaijan-Armenia war, would be widespread. This is not constrained to the land, but in an Indo-pacific context, could equally be applied to air and maritime environments. Development of extra-large unmanned underwater vehicles (XLUUVs) such as the US Navy Orca system opens the possibility of fully autonomous UUVs operating independently of crewed submarines and naval surface combatants, with the lower cost of such platforms allowing a greater number of systems, thus expanding the quantitative strength of naval forces.[42]

Rather than modern military technology driving armed forces towards more boutique and brittle force structures composed of fewer numbers of more complex and expensive platforms, the shift from 'platform-centric' paradigms to a 'system of systems' approach, employing networked force structures that include large numbers of autonomous weapons and systems seems to be emerging as a key indicator of the future shape of warfare. This idea is not new. As far back as the early 1990s, Martin C.

Libicki suggested the idea of 'Fire Ant Warfare' in which thousands of networked and autonomous microsensors and microprojectiles would overwhelm legacy systems.[43] The 'small, cheap and many' would overtake the 'large, expensive and few' on the future battlespace, challenging traditional approaches to capability development.

When considered against the broader trends implicit in a fourth industrial revolution (4IR) that incorporates rapid synthetic design and development and additive manufacturing (i.e., '3D Printing') technologies, the transformation in both the future shape of military forces, *and* the potential for disruptive innovation in terms of logistics and sustainment are undeniable. The development of the Loyal Wingman Airpower Teaming system in Australia is indicative of this change, taking only three years to go from a concept on paper to the first flight of the prototype.[44] The faster pace of development and production that is implicit in the use of autonomous systems, together with the prospect of lower cost of acquisition, heralds a period of disruptive innovation in military affairs, in which quantity rather than purely quality emerges as a source of military advantage.

The implications of Hypersonics

The speed advantage mentioned earlier is perhaps most significant in considering the impact of hypersonic weapons, which travel faster than five times the speed of sound (Mach 5 – 6,174km/h). China and Russia, as well as the United States, and others are pursuing a range of hypersonic missile systems.[45] Both China and Russia have operationally deployed hypersonic weapons, with China having deployed the DF-17 Hypersonic Glide Vehicle and has recently flown a hypersonic glide vehicle at global range in two fractional orbital bombardment system (FOBS) tests.[46] It is also testing advanced scramjet engines suitable for hypersonic cruise missiles that could be used in an antiship or land-attack role, and under Project *Tengyun*, is developing a fully reusable two stage to orbit hypersonic spaceplane.[47] This latter effort could transform Chinese space launch capability for rapid and responsive launch to enhance China's space resilience, and conversely, for offensive counterspace operations against US and allied space systems.

Andrew Davies notes that there's a long history of hypersonics research in Australia, dating back to the 1960s, much of it centred within the University of Queensland in cooperation with the Australian Defence Science and Technology group.[48] Australia possesses several hypersonic test facilities, including the Woomera test range, as well as aging but still effective hypersonic wind tunnels. He also notes that the 2020 Force

Structure Plan also included a reference to funding hypersonics research under the Southern Cross Integrated Flight Research Experiment (SCIFiRE).[49] He sums up Australia's potential future hypersonics capabilities, stating

> "Given Australia's in-country capability in hypersonics, there's an opportunity here for a rapid integration of newly developed hypersonic weapons into the force structure. The Defence Strategic Update notes that Australia's 'plans also include the acquisition of advanced air-to-air and strike capabilities with improved range, speed and survivability, potentially including hypersonic weapons… Australia isn't likely to want to acquire a global strike capability, but we're likely to be in the market for tactical hypersonic weapons to improve our strike capability, including anti-shipping weapons."[50]

The development of hypersonic weapons would certainly be in collaboration with the United States, emerging from SCIFiRE, with US efforts spread across several key projects.[51] The urgency to deploy hypersonic weapons, to match Chinese and Russian capabilities is likely to grow, given the potential impact such weapons will have on the future battlespace.

Hypersonic weapons compress decision time and extend tactical reach of missile capabilities. They demand early detection and tracking, ideally from space-based sensors, if terrestrial forces, such as naval vessels, are to have any chance of intercepting such weapons. The sheer speed of hypersonic weapons means that relying on local sensors would give virtually no time to intercept an incoming hypersonic weapon, rendering traditional forces such as aircraft carrier battlegroups highly vulnerable to attack.

There is debate over just how transformational hypersonic weapons will be in future warfare. The Chinese tests of their FOBS-HGV capability in late July and mid-August 2021, generated intense debate between those who argued that such a capability could potentially be seen as close to a 'Sputnik moment' against those who dismissed the significance of the capability.[52] The latter saw analysts citing the predominance of traditional ballistic missiles as a more effective delivery capability, and even challenging that the test was in fact an actual FOBS capability.[53] Advocates for the argument that hypersonic weapons will be transformational point to the weapons short time of flight that compresses a timeline for response, and its unpredictable flight path, evading ballistic missile defence systems. That short time of flight is of key importance given the potential for loss of political control over military forces, especially in an operational environment

that is also seeing intense counterspace, cyber and electromagnetic operations, and such a scenario raises the possibility of miscalculation leading to unintended escalation, especially if it is uncertain as to whether an incoming hypersonic weapon is carrying a nuclear or conventional warhead.

The US Missile Defense Review of 2019 highlights the critical role that space-based missile early warning and tracking play in countering hypersonic threats, such as air-breathing scramjet powered cruise missiles, as well as HGVs of the type recently tested by China in a FOBS profile.[54] In depending increasingly on space-based missile early warning and tracking which sits hundreds of kilometres above the visual or radar horizon, terrestrial missile defence systems have a better chance of detecting an incoming hypersonic threat, tracking it, and facilitating an interception of a missile. If the potential addition of directed-energy weapons (DEW) such as solid-state lasers are integrated, the combination of space-based missile early warning, missile interceptor systems, and DEW allows the best chance of defeating hypersonic threats. The risk facing such an effort is that adversary counterspace capabilities can be applied against these satellites to 'pluck out the eyes' of missile defence networks and cripple the ability of terrestrial forces to counter hypersonic threats. In effect, this increases the likelihood that space is not just an operational domain, but is a warfighting domain, from the outset of a future military conflict.

The Importance of the Space and Cyberspace Domains in future war

The examination of emerging themes of future warfare above – the importance of autonomous systems, the challenge of faster operational tempo for command and control, notions of swarming, and the role of hypersonics represent some of the most prominent aspects of debate on the character and conduct of future warfare. In addition to this capability-orientated analysis, the role of new operational domains, particularly space as an operational and warfighting domain, as well as cyberspace to attack critical information infrastructure, must be considered. There is also a blurring of these two domains, as the possibility of cyber attack on satellites and satellite ground stations emerges as a key challenge for space security.

Australia's elevation of space as an operational domain in the 2020 Force Structure Plan is a huge step forward in thinking compared to past white papers, which at best mentioned space briefly as an enabling environment for terrestrial forces, almost as if an afterthought, or worst, failed to address the importance of space at all. The shift parallels

a broader change in Australian thinking on space, both in terms of defence and national security, as well as civil and commercial aspects, that reflects a shift away from previous passive dependency on other states and commercial actors to provide a 'space segment' whilst Australia contributed a 'suitable piece of real estate' for ground facilities, towards becoming an active provider of sovereign space capability. The establishment of the Australian Space Agency in 2018, and the ADF Space Command from 2022 reinforces that Australia is now adopting a more sophisticated and ambitious perspective on space, including local development of space capabilities. With the growth of a commercial space sector, Australia is perhaps a year or two away from having the ability to launch Australian satellites on Australian launch vehicles from Australian launch sites on a regular basis.

For defence, this gives Australia the opportunity to enhance ADF capabilities in space, through key projects such as advanced satellite communications (Project JP-9102), sovereign geo-intelligence and earth observation (DEF-799 Phase 2), as well as space domain awareness (JP-9360), but also resilient positioning, navigation, and timing in a contested space domain (JP-9380), and most recently, a ground-based space electronic warfare capability (JP-9358).[55] This is a far cry from passive dependency and reflects a determination by Australia, and the growth of space capability, particularly emerging from an on-going space domain review to be finalised in 2022 is set to continue. The establishment of a sovereign launch capability in Australia is a key step, that will enable Australia to play a vital role in ensuring resilient space capabilities, both for the ADF and for key allies.

Space resilience is seen as vital given the contested nature of the space domain.[56] Australia can no longer assume assured access to vital space support in future war which will likely see increasing threats from adversary counterspace capabilities, and offensive use of ASATs.[57] Russia's recent test of a kinetic-kill ASAT reinforces the likelihood that in spite of the best of intentions on the part of international diplomatic and legal efforts, major powers will deploy counterspace capabilities, including a range of soft-kill systems, both space based and ground based, that are more usable than kinetic ASAT systems which leave clouds of space debris as an enduring challenge. The ground-based 'soft kill' systems include the prospect of cyber attack on satellites and on the ground segment, which could generate scalable and reversible effects via third-party non-state actors, offering an aggressor a degree of anonymity and deniability.

In future war, it is the combination of a rapid offensive counterspace campaign, directed against an opponent's vital space support systems – known as a 'space pearl harbour' – together with the offensive employment of cyber attacks on critical

information infrastructure – that are likely to represents the first shots of that war. Such measures also lend themselves to the prospect of grey zone operations, both in space and in cyberspace, at a level below that which would quickly justify a military response.[58] This use of grey zone operations allows offensive actions to occur even in peacetime, with Australia recently under cyber-attack from Chinese hackers launching cyber-attacks against Australia's Parliament.[59]

The increasing dependency on space and cyberspace for undertaking joint and integrated operations in the future battlespace will only accelerate the ADF's move towards deploying resilient space capabilities, and potentially even transitioning from a Defence Space Command towards an eventual Royal Australian Space Force in the more distant future, whilst the growth of Australia's offensive and defensive cyber capabilities is certain to continue.

Implications for the ADF in the Indo Pacific

In considering these themes of future warfare, and Australia's approach to addressing new military capabilities, its vital that the ADF, together with the Australian Defence organisation embrace new approaches not only to military operations but also capability acquisition. There is a risk that continued primacy of large, expensive platforms could erode our ability for innovative use of new types of technology, at the same time, starving the capability acquisition process of funding, skilled personnel, and political support for new capabilities. The greatest risk lies with autonomous systems, with a more cautious incremental approach to development of a range of advanced systems in the air, at sea and on land, hostage to legacy capabilities. In an operational sense, the risk is that of Libicki's 'Fire Ant Warfare' in which Australian ships, aircraft and ground forces are overwhelmed by adversary swarms of autonomous capabilities, many of which are directed not by humans on the loop, but through AI's making swifter tactical decisions than humans could possibly make. The ability of an adversary to strike rapidly at great range, using hypersonic weapons or advanced precision strike missiles, means that access to forward bases is at risk. That highlights the dangers of over-dependence on short-range crewed platforms, such as the F-35A Joint Strike Fighter, that now forms the core air combat capability for the RAAF. Lack of range confers an operational advantage to an adversary in a race to the swift – the side which strikes first, gains a decisive advantage. In future war in the Indo-pacific, this battle of the first salvo, be it in traditional domains, or in space and cyberspace, could well be decisive in shaping the outcome of conflict.

Australia's defence planners and strategic policy community are very aware of these challenges, and are seeking to address them, but face a serious challenge in changing ossified thinking within the Defence organisation on capability acquisition and overturning traditional paradigms regarding defence policy. The disconnect between the worsening strategic outlook facing Australia, against the outdated but still persistent 'steady as she goes' approach to capability acquisition is a serious risk to Australia's ability to meet future challenges that will occur in this decade and beyond. Australia makes a fine contribution to discussion about future warfare and future weapons, but many of its defence policy processes remain attuned to the last war. Addressing this policy gap and rapidly implementing new approaches to capability development and acquisition must be the most urgent priority for meeting future challenges. As noted above, the publication of strategy papers and concepts is not found lacking in Australia's defence policy community, and the defence organisation is very aware of the significance of new types of emerging military capability and new operational domains. Implementation of efforts to incorporate these new approaches to warfare is patchy in both organisational acceptance, and the pace of change. The risk posed by worsening US-China tensions, particularly over the possibility of a dangerous crisis across the Taiwan Straits perhaps in the second half of this decade means that Australia needs to accept change and recognise the importance of moving rapidly towards acquiring and deploying new types of military capabilities within the Indo-Pacific region.

[1] The Hon. Scott Morrison MP, Prime Minister of Australia, Launch of the 202 Defence Strategic Update, 1st July 2020, https://www.pm.gov.au/media/address-launch-2020-defence-strategic-update

[2] The Hon. Scott Morrison MP, Prime Minister of Australia, The Rt. Hon. Boris Johnson MP, Prime Minister of the United Kingdom, Joseph R. Biden Jr., President of the United States, Joint Leaders Statement on AUKUS, 16th September 2021, at https://www.pm.gov.au/media/joint-leaders-statement-aukus

[3] Department of Foreign Affairs and Trade, Joint Statement Australia – U.S. Ministerial Consultations (AUSMIN) 2021, September 16th 2021, at https://www.dfat.gov.au/geo/united-states-of-america/ausmin/joint-statement-australia-us-ministerial-consultations-ausmin-2021

[4] The Hon. Scott Morrison, MP, Prime Minister of Australia, Quad Leaders Summit Communique, 24th September 2021, at https://www.pm.gov.au/media/quad-leaders-summit-communique

[5] Ryan Hass, 'The "new normal" in US-China relations: Gardening competition and deep interdependence', The Brookings Institution, August 12th, 2021, at https://www.brookings.edu/blog/order-from-chaos/2021/08/12/the-new-normal-in-us-china-relations-hardening-competition-and-deep-interdependence/

[6] Rory Medcalf, Contest for the Indo-Pacific – Why China Won't Map the Future, La Trobe University Press, 2020, pp. 129-130.

[7] Graham Allison, 'What Xi Jinping Wants' *The Atlantic*, June 1st, 2017, at https://www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/

[8] Matthew Jamison, 'Countering China's Counter-Intervention Strategy', *The Strategy Bridge*, August 11th, 2020, at https://thestrategybridge.org/the-bridge/2020/8/11/countering-chinas-counter-intervention-strategy

[9] Joris Teer, Juliette Eijkelkamp, Paul can Hooft, 'China Outside the Western Pacific: Military Capabilities for Power Projection', in Joris Teer, Tim Sweijis, Paul van Hooft, Lotje Boswinkel, Juliette Eijkelkamp, and Jack Thompson, China's Military Rise and the Implications for European Security, The Hague Centre for Strategic Studies, November 2021, at https://hcss.nl/wp-content/uploads/2021/11/Chinas-Military-Rise-2021-Nov.pdf

[10] US Department of Defense, Military and Security Developments Involving the People's Republic of China 2021 – Annual Report to Congress, November 2021, pp. 126-127.

[11] Sam Rainsy, 'China's Cambodian Invasion', *The Strategist*, 5th August, 2019, at https://www.aspistrategist.org.au/chinas-cambodian-invasion/ ; Sam LaGrone, 'AFRICOM: Chinese Naval base in Africa Set to Support Aircraft Carriers', *USNI News*, April 2021 at

[12] H.R. McMaster, 'How China Sees the World', *The Atlantic*, May 2020, at https://news.usni.org/2021/04/20/africom-chinese-naval-base-in-africa-set-to-support-aircraft-carriers https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/ ; Gordon Lubold, Warren P. Strobel, 'Secret Chinese Port Project in Persian Gulf Rattles US Relations with U.A.E.', *The Wall Street Journal*, November 19th, 2021, at https://www.wsj.com/articles/us-china-uae-military-11637274224

[13] US China Economic and Security Review Commission, 2021 Report to Congress, 'Chapter 4 – Dangerous Period for Cross-Strait Deterrence: Chinese Military Capabilities and Decision-Making for a War over Taiwan', October 2021, at https://www.uscc.gov/annual-report/2021-annual-report-congress

[14] Brendan Nicholson, 'Dutton: War with China would be 'catastrophic' and mustn't be allowed to happen', *The Strategist*, 30th November 2021, at https://www.youtube.com/watch?v=cNP-E_XjetY&ab_channel=ABCNews%28Australia%29 ; see also The Hon. Peter Dutton MP, Minister of Defence, National Press Club Address, Canberra, 26th November 2021, at https://www.minister.defence.gov.au/minister/peter-dutton/speeches/national-press-club-address-canberra-act

[15] Department of Defence, 2020 Defence Strategic Update, 1.2, p. 11, https://www.defence.gov.au/about/publications/2020-defence-strategic-update

[16] Department of Defence, 1.12, p. 14

[17] Department of Defence, 1.13, p. 14
[18] Department of Defence, 1.8, p. 13
[19] Department of Defence, 1.9, p. 13
[20] Morrison, Johnson, Biden, Joint Leaders Statement on AUKUS, 16th September 2021, at https://www.pm.gov.au/media/joint-leaders-statement-aukus
[21] Department of Defence, 2020 Force Structure Plan, 6.8-6.9, pp. 62-63, https://www.defence.gov.au/about/publications/2020-force-structure-plan
[22] Malcolm Davis, 'ADF space command is the right next step for Australian space power', *The Strategist*, 5th May 2021, at https://www.aspistrategist.org.au/adf-space-command-is-the-right-next-step-for-australian-space-power/
[23] Marcus Hellyer, Delivering a stronger Navy, faster, ASPI, 2nd November 2021, at https://www.aspi.org.au/report/delivering-stronger-navy-faster ; Andrew Davies, 'Nuclear or bust: Our high-risk submarine plan', in *The Weekend Australian – Defence Supplement*, October 30th-31st, 2021, p.18
[24] John Coyne, Matthew Page, 'Are Australia's new armoured vehicles too heavy?', *The Strategist*, 4th June 2021, at https://www.aspistrategist.org.au/are-australias-new-armoured-vehicles-too-heavy/
[25] Department of Defence, 2020 Force Structure Plan, 4.6, 5.8, p. 36, p. 51.
[26] Malcolm Davis, ' AUKUS: looking beyond the submarines', *The Strategist*, 4th November 2021, at https://www.aspistrategist.org.au/aukus-looking-beyond-the-submarines/
[27] The Hon. Scott Morrison MP, The Prime Minister, Sovereign Guided Weapons Manufacturing, 31st March 2021, at https://www.pm.gov.au/media/sovereign-guided-weapons-manufacturing
[28] Malcolm Davis, Forward Defence in Depth for Australia, June 2019, ASPI Strategic Insights, at https://www.aspi.org.au/report/forward-defence-depth-australia
[29] Department of Defence, 2020 Defence Strategic Update, pp. 25 – 29.
[30] David S Fadok, USAF, John Boyd and John Warden – Air Power's Quest for Strategic Paralysis, Air University Press, February 1995, p. 16.
[31] Department of Defence, MQ-4c Triton Unmanned Aircraft System, https://www.airforce.gov.au/technology/aircraft/intelligence-surveillance-and-reconnaissance/mq-4c-triton-unmanned-aircraft; Department of Defence, AIR 7003 Phase 1 MQ-9B Sky Guardian Remotely Piloted Aircraft System, https://www.defence.gov.au/project/air7003-skyguardian-armed-remotely-piloted-aircraft-system
[32] Boeing, Boeing Airpower Teaming System, https://www.boeing.com/defense/airpower-teaming-system/
[33] Department of Defence, Autonomous Warrior enhances Navy's fighting edge, 9th June 2021, https://news.defence.gov.au/technology/autonomous-warrior-enhances-navys-fighting-edge
[34] Peter W. Singer, Wired for War – The Robotics Revolution and Conflict in the 21st Century, Penguin, New York, 2009, pp. 124-128; Paul Scharre, Army of None – Autonomous Weapons and the future of War, W.W.Norton & Co, New York, 2018, pp 251-270.
[35] Royal Australian Navy, RAS-AI Strategy 2040, https://www.navy.gov.au/media-room/publications/ras-ai-strategy-2040
[36] Department of Defence, HACSTRAT – A strategic approach for air and space capability, 2021, p. 8 https://www.airforce.gov.au/our-mission/hacstrat
[37] Department of Defence, p. 9
[38] Department of Defence, p. 24.
[39] Department of Defence, ADF Concept for Future Robotics and Autonomous Systems, 2020, https://defence.gov.au/vcdf/forceexploration/adf-concept-future-robotics-autonomous-systems.asp ; Australian Army, Robotics and Autonomous Systems Strategy, 2018, https://researchcentre.army.gov.au/library/other/robotic-autonomous-systems-strategy
[40] Department of Defence, 2020, p. 9
[41] Malcolm Davis, 'Cheap drones versus expensive tanks: a battlefield game changer?', *The Strategist*, 21st October 2020, at https://www.aspistrategist.org.au/cheap-drones-versus-expensive-tanks-a-battlefield-game-changer/

[42] Malcolm Davis, 'AUKUS requires rapid expansion of autonomous undersea warfare system', *The Australian*, 30th October 2021, https://www.aspi.org.au/opinion/aukus-requires-rapid-expansion-autonomous-undersea-warfare-systems

[43] Martin C. Libicki, The Mesh and the Net – Speculations on Armed Conflict in a Time of Free Silicon, McNair Paper 28, Institute for National Strategic Studies, March 1994.

[44] Malcolm Davis, 'Loyal Wingman leads the way to the RAAF of 2121', *The Strategist*, 5th March 2021, https://www.aspistrategist.org.au/loyal-wingman-leads-the-way-to-the-raaf-of-2121/

[45] Andrew Davies, Coming Ready or Not: Hypersonic weapons, ASPI, March 2021, https://www.aspi.org.au/report/coming-ready-or-not-hypersonic-weapons

[46] Malcolm Davis, 'Can US missile-defence systems handle China's new missiles?' *The Strategist*, 27th October 2021, https://www.aspistrategist.org.au/can-us-missile-defence-systems-handle-chinas-new-missiles/

[47] Jean Deville, 'China's Spaceplane Projects: Past, Present and Future', *The China Aerospace Blog*, May 11th 2020, https://china-aerospace.blog/2020/05/11/chinas-spaceplane-projects-past-present-and-future/

[48] Andrew Davies, 2021, pp. 6-7.

[49] Andrew Davies, 2021, p. 7; also Department of Defence, 2020 Force Structure Plan, 5.8, p. 51, https://www.defence.gov.au/about/publications/2020-force-structure-plan; Royal Australian Air Force, SCIFire Hypersonics, https://www.airforce.gov.au/our-mission/scifire-hypersonics

[50] Andrew Davies, 2021, p. 7.

[51] Congressional Research Service, Hypersonic Weapons: Background and Issues for Congress, R45811, 19th October 2021, pp. 4 – 8, https://crsreports.congress.gov/product/pdf/R/R45811

[52] David E. Sanger, William J. Broad, 'China's Weapon Tests Close to a "Sputnik Moment," U.S. General says" *New York Times*, October 27th, 2021, https://www.nytimes.com/2021/10/27/us/politics/china-hypersonic-missile.html

[53] Bleddyn Bowen, Cameron Hunter, Chinese Fractional Orbital Bombardment, APLN Policy Brief, No. 78, 1st November 2021, https://apln.network/analysis/policy-briefs/chinese-fractional-orbital-bombardment;

[54] US Department of Defense, 2019 Missile Defense Review, p. 36, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF

[55] The Hon. Peter Dutton MP, Minister of Defence, 'Defence explores options for Space Electronic Warfare', 29th July 2021, https://www.minister.defence.gov.au/minister/peter-dutton/media-releases/defence-explores-options-space-electronic-warfare ; Malcolm Davis, 'Australia needs a national space strategy' *The Strategist*, 25th August 2021, https://www.aspistrategist.org.au/australia-needs-a-national-space-strategy/

[56] Malcolm Davis, 'Defence to examine plans for space domain', *The Australian*, 22nd May 2021, https://www.aspi.org.au/opinion/defence-examine-plans-space-domain

[57] Malcolm Davis, The Australian Defence Force and contested space, ASPI, August 2019, https://www.aspi.org.au/report/australian-defence-force-and-contested-space

[58] Todd Harrison, Kaitlyn Johnson, Makena Young, Defense against the Dark Arts in Space: Protecting Space Systems from counterspace weapons, CSIS, 25th February 2021, https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons

[59] Reuters, 'Australia concluded China was behind hack on parliament, political parties', 16th September 2019, https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF

Chapter 6
The AI Wave in Military Affairs: Enablers and Constraints

Michael Raska

In the 2020s, debates in strategic studies increasingly focus on the impact of emerging technologies on defense innovation and future character of warfare. The convergence of advanced novel technologies such as artificial intelligence (AI) systems, robotics, additive manufacturing (or 3D printing), quantum computing, directed energy, and other 'disruptive' technologies, defined under the commercial umbrella of the 4th Industrial Revolution (4IR), promises new and potentially significant opportunities for defense applications and, in turn, for increasing one's military edge over potential rivals. Much of the current debate arguably portrays the "next-frontier" technologies as synonymous with a "discontinuous" or "disruptive" military innovation in the character and conduct of warfare - from the "industrial-age" toward "information-age warfare" and now increasingly toward "automation-age warfare" (Raska, 2021). For example, advanced sensor technologies such as hyperspectral imagery, computational photography, and compact sensor design aim to improve target detection, recognition, and tracking capabilities and overcome traditional line-of-sight interference (Freitas et al., 2018). Advanced materials such as composites, ceramics, and nanomaterials with adaptive properties will make military equipment lighter but more resistant to the environment (Burnett et al., 2018). Emerging photonics technologies, including high-power lasers and optoelectronic devices, may provide new levels of secure communications based on quantum computing and quantum cryptography (IISS, 2019).

The convergence of emerging technologies – i.e. robotics, artificial intelligence and learning machines, modular platforms with advanced sensor technologies, novel materials and protective systems, cyber defenses and technologies that blur the lines between the physical, cyber, and biological domains, is widely seen as having profound implications on the character of future warfare. For modern militaries, the application of novel machine-learning algorithms to diverse problems also promises to provide unprecedented capabilities in terms of speed of information processing, automation for a mix of manned/unmanned weapons platforms and surveillance systems, and ultimately, command and control (C2) decision-making (Horowitz, 2018; Cummings, 2017).

Notwithstanding the varying strategic contexts, however, the diffusion of these

emerging technologies is also prompting theoretical and policy-prescriptive questions similar to those posed over the past four decades: Does the diffusion of emerging technologies really signify a 'disruptive' shift in warfare, or is it a mere evolutionary change? If emerging technologies stipulate a disruptive change in warfare, what are defense resource allocation imperatives, including force structure and weapons procurement requirements? How can military organizations, including air forces, exploit emerging technologies to their advantage? Furthermore, how effective are emerging technologies to counter security threats and challenges of the 21st century, characterized by volatility, uncertainty, complexity, and ambiguity?

Four Decades of Disruptive Narratives

Driven largely by the quantum leaps in information technologies, the trajectory of 'disruptive' military innovation narratives and debates have been defined in the context of IT-driven Revolution in Military Affairs (IT-RMA), which have progressed through at least five stages: (1) the initial conceptual discovery of the Military-Technical Revolution by Soviet strategic thinkers in the early 1980s, (2) the conceptual adaptation, modification, and integration in the US strategic thought during the early 1990s, (3) the technophilic RMA debate during the mid-to-late 1990s, (4) a shift to the broader "defense transformation" and its partial empirical investigation in the early 2000s, and (5) critical reversal questioning the disruptive narrative from 2005 onwards (Gray, 2006). Since the mid-2010s, however, with the accelerating diffusion of novel technologies such as AI and autonomous systems, one could argue that a new AI-RMA – or the sixth RMA wave - has emerged (Raska, 2021).

In retrospect, however, the implementation of IT-RMA over the past four decades has also arguably followed a distinctly less than revolutionary or disruptive path, consisting of incremental, often near-continuous, improvements in existing capabilities (Ross, 2010). While major, large-scale, and simultaneous military innovation in defense technologies, organizations, and doctrines have been a rare phenomenon, military organizations have largely progressed through a *sustained* spectrum of military innovations ranging from small-scale to large-scale innovation that shaped their conduct of warfare (Goldman, 1999). While many military innovations during this era, such as concepts of Network-Centric Warfare, have matured, the ambitious narratives of impending 'disruptive military transformation' have nearly always surpassed available technological, organizational, and budgetary capabilities. Moreover, the varying conceptual, technological, organizational,

and operational innovations focused primarily on integrating digital information technologies into *existing* conventional platforms and systems (Raska, 2016).

For example, in the US strategic thought, the narratives of disruptive military innovation have gradually waned from 2005 onwards with operational challenges and experiences in wars in Iraq and Afghanistan. More critical voices pointed toward unfulfilled promises of 'disruptive' defense transformations. The rationale for 'new way of thinking and a new way of fighting' justifying virtually every defense initiative or proposal, signaled disorientation rather than a clear strategy (Freedman, 2006). Defense transformation sceptics also cautioned about the flawed logic in solving complex strategic challenges through technology, while discarding the adaptive capacity of potential enemies or rivals. In short, disruptive narratives of impending defense transformations have turned into an ambiguous idea, propelled by the budgetary requirements and unrealistic capability sets rather than actual strategic and operational logic (Reynolds, 2006).

Why the AI-Wave Differs?

The new 'AI-enabled' defense innovation wave, however, differs from the past IT-led waves in several ways. First, the diffusion of AI-enabled military innovation proceeds at a much faster pace, through multiple dimensions, notably through the accelerating geostrategic competition between great powers - the United States, China, and to a lesser degree Russia. Strategic competitions between great powers are not new; they have been deeply rooted in history – from the Athenian and Spartan grand strategies during the Peloponnesian War in the fifth century BCE, to the bipolar divide of the Cold War during the second half of the twentieth century. The character of the emerging strategic competition, however, differs from analogies of previous strategic competitions. In the 21st century, the paths and patterns of strategic competitions are more complex and diverse, reflecting multiple competitions under different or overlapping sets of rules in which long-term economic interdependencies co-exist with core strategic challenges (Lee, 2017). In a contest over future supremacy, however, technological innovation is portrayed as a central source of international influence and national power - generating economic competitiveness, political legitimacy, and military power (Mahnken, 2012). Specifically, for the first time in decades, the US faces a strategic peer competitor, China, capable of pursuing and implementing its own AI-RMA. Accordingly, the main question is not whether the AI-RMA wave is 'the one' that will bring about a fundamental

discontinuity in warfare, and if so, how and why? Instead, it is whether the US AI-RMA can be nullified – or at least weakened – by corresponding Chinese or Russian AI-RMAs? In other words, the margins of technological superiority are effectively narrowing, which effectively accelerates the strategic necessity for novel technologies as a source of military advantage.

Second, contrary to previous decades, which, admittedly, utilized *some* dual-use technologies to develop major weapons platforms and systems, the current AI-enabled wave differs in the magnitude and impact of the commercial-technological innovation as the source of military innovation (Raska, 2020). Large military-industrial primes are no longer the only drivers of technological innovation; instead, advanced technologies with a dual-use potential are being developed in the commercial sectors and then being 'spun on' to military applications. In this context, the diffusion of emerging technologies, including additive manufacturing (3D printing), nanotechnology, space and space-like capabilities, artificial intelligence, and drones, are not confined solely to the great powers (Hammes, 2016). The diffusion of AI-enabled sensors and autonomous weapon systems is also reflected in defense trajectories of select advanced small states and middle powers such as Singapore, South Korea, Israel, and others. These have now the potential to develop niche emerging technologies to advance their defense capabilities and their economic competitiveness, political influence, and status in the international arena (Barsade and Horowitz, 2018).

Third, the diffusion of autonomous and AI-enabled autonomous weapons systems, coupled with novel operational constructs and force structures, challenge the direction and character of human involvement in future warfare – in which algorithms may shape human decision-making, and future combat is envisioned in the use of Lethal Autonomous Weapons Systems (LAWS). Advanced militaries, including air forces, are experimenting with varying man-machine technologies that rely on data analytics and automation in warfare. These technologies are increasingly permeating future warfare experimentation and capability development programs (Jensen and Pashkewitz, 2019). In the US, for example, select priority research and development areas focus on the development of AI-systems and autonomous weapons in various human-machine type collaborations – i.e. AI-enabled early warning systems and command and control networks, space and electronic warfare systems, cyber capabilities, lethal autonomous weapons systems, and others.

The convergence of the three drivers - strategic competition, dual-use emerging technological innovation, and changing character of human-machine interactions

in warfare propel a new set of conditions that define the AI-RMA wave. Its diffusion trajectory inherently also poses new challenges and questions concerning strategic stability, alliance relationships, arms control, ethics and governance, and ultimately, the conduct of combat operations (Stanley-Lockman, 2021a). International normative debates on the role of AI systems in the use of force, for example, increasingly focus on the diffusion of LAWS and the ability of states to conform to principles of international humanitarian law. As technological advancements move from the realm of science fiction to technical realities, states also have different views on whether the introduction of LAWS would defy or reinforce international legal principles. Facing contending legal and ethical implications of military AI applications, military establishments increasingly recognize the need to address questions related to safety, ethics, and governance, which are crucial to building trust in new capabilities, managing risk escalation, and revitalizing arms control. Still, there is a tension between how much defense ministries and militaries focus their ethics efforts narrowly on LAWS or more broadly on the gamut of AI-enabled systems. Hence, military organizations need to track the evolving perspectives on AI and autonomy and debates on implications to the strategic and operational environment of the 2020s and beyond (Stanley-Lockman, 2021b).

Application of the AI Wave in Airpower

At the operational level, for example, the application of AI-wave can be seen in changing conceptions of airpower. Modern air forces aim to accelerate the integration of varying AI-related systems and technologies such as multi-domain combat cloud systems, which collect big-data from a variety of sources, creating a real-time operational picture, and essentially, automate and accelerate command and control (C2) processes (Robinson, 2021). For example, AI-enabled combat clouds are posed to identify targets and allocate them to the most relevant "shooters" in any domain, whether airborne, surface or underwater – which some air forces conceptualize as Joint All-Domain Command and Control (JADC2). Select air forces such are also experimenting with AI algorithms as 'virtual backseaters', which effectively control the aircraft's sensors and navigation, finding adversary targets, and in doing so, reduce the aircrew's workload (Everstine, 2020).

In this context, the key argument is that advances in AI systems – broadly programs that can sense, reason, act, and adapt, including Machine Learning (ML) systems - algorithms whose performance improves with increasing data interactions over time, and Deep Learning (DL) systems - in which multilayered neural networks learn from vast

amounts of data – have the potential "to transform air combat operations and the way airpower is conceived and used" (Davis, 2021). According to a RAND study (Lingel et al., 2020), there are currently six categories of applied AI/ML research and development that have implications for future warfare, including airpower:

(1) Computer vision - image recognition - detecting and classifying objects in the visual world that could be used to process multisource intelligence and data fusion;
(2) Natural language processing (NLP) - ability to successfully understand human speech and text recognition patterns, including translation, that could be used to extract intelligence from speech and text, but also monitor friendly communications and direct relevant information to alert individuals or units in need;
(3) Expert systems or rule-based systems - collecting large amounts of data to recommend particular actions to achieve operational and tactical objectives;
(4) Planning systems - using data to solve scheduling and resource allocation problems, which could coordinate select air, space, and cyber assets against targets and to generate recommended time-phased actions;
(5) Machine learning systems - acquiring knowledge from data interactions with the environment, which could be used in conjunction with other categories of AI, i.e. to enable C2 systems to learn how to perform tasks when expert knowledge is not available or when optimal tactics, techniques, and procedures (TTPs) are unknown;
(6) Robotics and autonomous systems - combining AI/ML methods from all or select preceding categories that would enable unmanned systems interactions with their environment;

These AI-related categories are applicable into nearly every aspect of airpower, potentially shaping new forms of automated warfare: from C2 decision support and planning, in which AI/ML could provide recommended options or proposals in increasingly constrained times; ISR support through data mining capabilities; logistics and predictive maintenance to ensure the safety of forces and availability of platforms and units; training and simulation; cyberspace operations to detect and counter advanced cyber-attacks; robotics and autonomous systems such as drones that are utilized across various missions from ISR to the tip of the spear missions such as suppression of enemy

air defenses and collaborative combat that integrates the varying manned and unmanned platforms in air and land strike operations. In other words, the argument here is that AI systems will be increasingly capable to streamline C2 and decision-making processes in every step of the John Boyd's Observe-Orient-Decide-Act (OODA) loop: collecting, processing, and translating data into a unified situational awareness view, while providing options for a recommended course of actions, and ultimately, helping humans to act (Fawkes and Menzel, 2018).

From Defense to Military Innovation: Ongoing Challenges

However, integrating AI systems into military platforms, systems, and organizations to transform computers from tools into problem-solving "thinking" machines will continue to present a range of complex technological, organizational, and operational challenges (Raska et al, 2021). These may include developing algorithms that will enable these systems to better adapt to changes in their environment, learn from unanticipated tactics and apply them on the battlefield. It would also call for designing ethical codes and safeguards for these thinking machines. Another challenge is that technological advances, especially in military systems, are a continuous, dynamic process; breakthroughs are always occurring, and their impact on military effectiveness and comparative advantage could be significant and hard to predict at their nascent stages. Moreover, such technologies and resulting capabilities rarely spread themselves evenly across geopolitical lines.

Most importantly, however, the critical question is how much we can trust AI systems, particularly in the areas of safety-critical systems? As Missy Cummings warns, "history is replete with examples of how similar promises of operational readiness ended in costly system failures and these cases should serve as a cautionary tale" (Cummings, 2021). Furthermore, a growing field of research focuses on how to deceive AI systems into making wrong predictions by generating false data. Both state and non-state actors may use this so-called adversarial machine learning to deceive opposing sides, using incorrect data to generate wrong conclusions, and in doing so, alter the decision-making processes. The overall strategic impact of adversarial machine learning on international security might be even more disruptive than the technology itself (Knight, 2019; Danks, 2020).

From a tactical and operational perspective, many of these complex AI systems also need to be linked together – not only technologically but organizationally and operationally. For many militaries, this is an ongoing challenge - they must be able to

effectively (in real-time) integrate AI-enabled sensor-to-shooter loops and data streams between the various services and platforms. This means effectively linking the diverse Air Force, Army, Navy, and Cyber battle management systems and data; command and control, communications and networks; ISR; electronic warfare; positioning, navigation, and timing; with precision munitions. While select AI/ML systems may mitigate some of the challenges, the same systems create another set of new problems related to ensuring trusted AI. Accordingly, one may argue that the direction and character of AI trajectories in military affairs will depend on corresponding strategic, organizational and operational agility, particularly how these technologies interact with current and emerging operational constructs and force structures.

Going forward, the level of human involvement in the future of warfare, the need to alter traditional force structures and recruitment patterns and in what domains force will be used are all matters that are being challenged by new technologies. Modern militaries are developing their own and often diverse solutions to these issues. As in the past, their effectiveness will depend on many factors that are linked to the enduring principles of *strategy* – the ends, ways, and means to "convert" available defense resources into novel military capabilities, and in doing so, create and sustain operational competencies to tackle a wide range of contingencies. The main factors for successful implementation will not be technological innovations per se, but the combined effect of sustained funding, organizational expertise (i.e. sizeable and effective R&D bases, both military and commercial) and institutional agility to implement defense innovation (Cheung, 2021). This means broadly having the people, processes and systems capable of delivering innovative solutions, while maintaining existing core capabilities that would provide viable policy options in an increasingly complex strategic environment.

Bibliography:

Barsade, I. and Horowitz, M. 2018. Artificial intelligence beyond the superpowers. *Bulletin of the Atomic Scientists*. 16 August. Available from: https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/

Burnett, M. et. al. 2018. Advanced materials and manufacturing - implications for defence to 2040. *Defence Science and Technology Group Report*. Australia Department of Defence. Available from: https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-GD-1022.pdf

Cheung, T. 2021. A conceptual framework of defence innovation. *Journal of Strategic*

Studies, DOI: 10.1080/01402390.2021.1939689.

Cummings, M. 2017. Artificial intelligence and the future of warfare. *Chatham house research paper*. 26 January. Available from: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf

Cummings, M. 2021. Rethinking the maturity of artificial intelligence in safety-critical settings. *AI Magazine*, 42(1), pp.6-15. Available from: https://ojs.aaai.org/index.php/aimagazine/article/view/7394

Danks, D. 2020. How adversarial attacks could destabilize military AI systems. *IEEE Spectrum*. 26 February. Available from: https://spectrum.ieee.org/adversarial-attacks-and-ai-systems

Davis, M. 2021. The artificial intelligence 'backseater' in future air combat. *ASPI Strategist*, 5 February. Available from: https://www.aspistrategist.org.au/the-artificial-intelligence-backseater-in-future-air-combat/

Everstine, B. 2020. U-2 flies with artificial intelligence as its co-pilot. Air Force Magazine, 16 December. Available from: https://www.airforcemag.com/u-2-flies-with-artificial-intelligence-as-its-co-pilot/

Fawkes, J. and Menzel, M. 2018. The future role of artificial intelligence - military opportunities and challenges. *The Journal of the JAPCC*, 27. pp.70-77. Available from: https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf

Freedman, L. 2006. *The transformation of strategic affairs*. London: International Institute of Strategic Studies.

Freitas, S. Silva, H., Almeida, J. and Silva, E. 2018. Hyperspectral imaging for real-time unmanned aerial vehicle maritime target detection. *Journal of Intelligent and Robotic Systems*. 90, pp.551-570.

Goldman, E. 1999. Mission possible: organizational learning in peacetime. In: Trubowitz, P., Goldman, E., and Rhodes, E. *The politics of strategic adjustment: ideas, institutions, and interests*. New York: Columbia University Press, pp.233-266.

Gray, C. 2006. *Strategy and history: essays on theory and practice*. London: Routledge, pp.113-120.

Hammes, T.X. 2016. Technologies converge and power diffuses: the evolution of small, smart, and cheap weapons. *CATO Institute Policy Analysis*. 786, 27 January. Available from: https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons

Horowitz, M. 2018. The promise and peril of military applications of artificial

intelligence. *Bulletin of the Atomic Scientists*. 23 April. Available from: https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/

International Institute for Strategic Studies. 2019. Quantum computing and defence. In: IISS. *The military balance*. London: Routledge, pp. 18-20.

Jensen, B. and Pashkewitz, J. 2019. Mosaic warfare: small and scalable are beautiful. *War on the Rocks*. 23 December. Available from: https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/

Knight, W. 2019. Military artificial intelligence can be easily and dangerously fooled. MIT Technology Review. 21 October. Available from: https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/

Lee, CM.2016. *Fault lines in a rising Asia*. Washington DC: Carnegie Endowment for International Peace, pp. 119-175. Available from: https://carnegieendowment.org/2016/04/20/fault-lines-in-rising-asia-pub-63365

Lingel, S. et. al. 2020. Joint all-domain command and control for modern warfare - an analytic framework for identifying and developing artificial intelligence applications. *RAND Corporation Project Air Force Report*. Available from: https://www.rand.org/pubs/research_reports/RR4408z1.html

Mahnken, T. (ed.). 2012. *Competitive strategies for the 21st century: theory, history, and practice*. Stanford: Stanford University Press, pp.3-12.

Raska, M. 2016. *Military innovation in small states: creating a reverse asymmetry*. New York: Routledge. Available from: https://www.routledge.com/Military-Innovation-in-Small-States-Creating-a-Reverse-Asymmetry/Raska/p/book/9780367668617

Raska, M. 2020. Strategic competition for emerging military technologies: comparative paths and patterns. *Prism – Journal of Complex Operations*. 8(3), pp.64-81. Available from: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf

Raska, M. 2021. The sixth RMA wave: disruption in military affairs? *Journal of Strategic Studies*. 44(4), pp.456-479.

Raynolds, K. 2006. *Defence transformation: to what? for what?* Carlisle: Strategic Studies Institute.

Robinson, T. 2021. The air force of 2040 – synthetically-trained, cloud-networked, space-enabled and NetZero? Royal Aeronautical Society, 10 August. Available from: https://www.aerosociety.com/news/the-air-force-of-2040-synthetically-trained-cloud-networked-space-enabled-and-netzero/

Ross, A. 2010. On military innovation: toward an analytical framework. *IGCC Policy Brief*. 1, pp.14-17. Available from: https://escholarship.org/uc/item/3d0795p8

Stanley-Lockman. Z. 2021(a). Responsible and ethical military AI: allies and allied perspectives. *Center for Security and Emerging Technology Issue Brief*. 25 August. Available from: https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/

Stanley-Lockman, Z. 2021(b). Military AI cooperation toolbox: modernizing defense science and technology partnerships for the digital age. *Center for Security and Emerging Technology Issue Brief*. 25 August. Available from: https://cset.georgetown.edu/publication/military-ai-cooperation-toolbox/

Chapter 7
The U.S.-China Tech War: A Dawn of New Geopolitics?

Ivan V. Danilin

In 2019 Donald Trump enacted first systematic sanctions against Huawei and ZTE – officially, to stop further expansion of Chinese technologies and standards for 5G telecommunication systems positioned by the White House as "insecure" and supporting Beijing's espionage capabilities. This step initialized process that was later labeled by some exerts as a "Technology War" (or shortly "The Tech War") – in association with the U.S.-China trade war that started in 2018 (Sun, 2019; Chang, 2020; Barkin, 2020; Danilin, 2020; Zhao, 2021). However, this new technology conflict may be rebranded as "Digital War" since it is focused on wide range of information and communication technologies (ICT): microelectronics, semiconductor manufacturing systems, telecommunication equipment, supercomputers, specialized software and internet solutions. An important separate accent is placed on digital technologies labeled by experts and media as emerging, disruptive, or transformative, like Artificial Intelligence (AI) and quantum computing that are seen as basic for the future markets and tech power.

Sharpened by rising political and security tensions, the Tech War enforced and reshaped ongoing changes in the U.S.-China relations (and with the West in general) with multiple global and regional (Asian and European) strategic implications. What is not less important, it seems that the Tech War marked new realm of the global politics – now seen also in Russia-West confrontation. Thus, understanding the Tech War, from its formal driving forces to political economy, is necessary for understanding not only U.S.-China relations, but also regional and global trends and future challenges.

The Economic Landscape of the Tech War

The fact that digital markets and information and communication technologies moved into the focus of a new economic conflict is both unsurprising and shockingly unexpected.

During last decades ICT evolved as key driving forces of global development, trade, and Post-Cold War globalization. Different OECD, UNCTAD and other studies

illustrate how ICT – and Internet in first place – drive GDP growth and qualitative changes in national economies by enhancing entrepreneurial activity, rise of labor productivity, supporting exports and other important economic and social processes (see, for example: UNCTAD, 2019; OECD, 2020). ICT are also important for the global trade and investments – outside of intensive use of digital technologies in financial sector and logistics. By different calculations, ICT are responsible for up to 12% of global exports in goods and approximately 11% in services – including more than 60% of the high-tech exports and about 20% of trade in knowledge-intensive services (OECD, 2020; National Science Board, 2020; The World Bank, 2021). Global electronic industry also played an important role in sharp rise of the Foreign Direct Investments (FDI) since 1990s.

These processes gained additional impetus in 2010s from the "smartphone revolution" and associate rise of the Internet – ICT-driven – global markets like e-commerce and social media, advancing the Digital Economy realm. By different calculations its size ranges from 4% ("narrow" definition – Internet markets with supportive ICT goods and services) and up to 25-30% (all ICT markets plus effects induced in other industries) of the global GDP (Barefoot et al., 2018; International Monetary Fund, 2018; UNCTAD, 2019).

Highly internationalized nature of the ICT markets and value chains was and still is promoted by strong global demand, differences in production costs, deepening specialization in production and research and development (R&D). All these factors are explained by a complex combination of the market forces and developmental efforts of different nation states to nurture prospective digital industries since 1970s. Modern production of ICT goods is geographically fragmented, but highly coordinated. ICT global value chains (GVC) are mostly concentrated in top-10 counties (United States, Japan, Republic of Korea, P.R.C., etc.), but different functions and centers of excellence are located almost everywhere, from Germany to Brazil, and from Singapore to Russia (UNCTAD, 2019). It is even more true for supportive businesses, not always integrated in corporate GVCs, like development of online games. Here we can see some unexpected locations like Belarus (Minsk High Technology Park).

ICT are also responsible for the important part of global innovations. If measured in most valuable patent families (registered in at least 2 of top-5 jurisdictions[1]) in

[1] U.S. Patent and Trademark Office, European Patent Office, Japan Patent Office, Korean Intellectual Property Office, and the National Intellectual Property Administration of People's Republic of China

2014-2017 globally ICT were responsible for 35,3% of all registered patents (OECD 2020). And this is not to mention wide use of different digital technologies in R&D, design, and other innovation-related activities. ICT and Internet businesses (also related to the non-digital industries like healthcare or education) are also key area of the global venture investments (Pitchbook, 2020; National Venture Capital Association, 2021; KPMG, 2021).

And in the long term, further rise of the ICT's role in the global economy is inevitable, especially considering Internet of Everything and AI as almost classic general purpose technology (Jovanovic and Rousseau, 2005; Bresnahan, 2010).

The role of the ICT is especially important when we analyze Chinese and American economies and bilateral economic relations.

In China, ICT supports more than 30% of the nation's export of goods (around 40% of the global ICT exports), making it an important source of revenues (National Science Board, 2020; World Bank, 2021). It is also a critical factor of internal development considering both ongoing digitalization of Chinese economy[2] and the fact that digital industries were and still are the most innovative sector of the P.R.C. economy. Quite predictably, China is trying to strengthen its potential in most advanced digital areas also considering its implications for traditional hard power.

In turn, the U.S.A. was always emphasizing ICT as one of its globally most competitive industries and important part of national economy (up to 10% or more considering both traditional ICT and internet markets with profound economic impact on other industries). America still has strong market positions (up to 50-100% of global sales) in some most technologically advanced areas, from operating systems to the most sophisticated electronic components (UNCTAD, 2019; Semiconductor Industry Association, 2020; OECD, 2020). U.S.A. also leads in digital venture activities, as well as in research and development efforts (National Science Board, 2020; National Venture Capital Association, 2021). The industry was always seen as strategic for both economic development and defense, as was well shown by activities of CoCom and the U.S.-Japan relations in 1980s (see below).

Importance of the ICT for both nations predefined dialectic nature of their digital interactions.

---

[2] On different activities related to development and scaling-up of internet technologies in the P.R.C. see, for example, official web-page of the Chinese national program "Internet Plus" (English version of the web-site of the State Council of the People's Republic of China: https://english.www.gov.cn/2016special/internetplus/).

On one hand, China's ambitions are focused at re-mastering GVC architecture and redistribution of the global value add in the digital sector, while for the United States maintaining its technological dominance is critical for market power. Both nations are also aiming at future disruptive digital technologies and markets that are important for economic growth and global leadership.

On the other, even setting aside consumer electronic exports, China and the United States are closely intertwined in the digital area. Despite China is seen as an electronic powerhouse, it is still very dependent on key U.S. and other Western technologies, from high-performance chips and up to semiconductor manufacturing equipment. It is well illustrated by the sizeable P.R.C. imports of microelectronics (up to 60% of world's total) with only about 15% of the needed components produced in the Mainland China (mostly less sophisticated ones) (Semiconductor Industry Association, 2020; IC Insights, 2021; Xi, 2021; Thomas, 2021; Grimes and Du, 2022). Chinese companies also use Windows, Android, and other American software and only now seem to develop alternatives. For many American businesses, in turn, Chinese market is important (Apple, Microsoft and others) or even the biggest one (e.g., for Qualcomm or Texas Instruments). R&D and other innovation cooperation is important too – especially for giants like Google and Intel or Huawei and BOE Technology Group. For the U.S. companies, Chinese growing S&T sector is a new source of talents and other inputs by reasonable price, while for the P.R.C. advanced American competences and technologies are critical for development.

This digital dualism illustrates the Tech War dilemma.

Considering future markets and global leadership at stake, some kind of conflict over ICT markets seemed to be structurally inevitable. However, the Tech War as an ultimate form of it was not unavoidable or predictable. GVC in the digital area with all its flexibility were and still are structurally very interdependent, ICT markets are necessarily global, while production and innovation activities of both U.S.A. and China are increasingly interconnected. So, hypothetically in some "ideal futures" the two nations may have been complementary competitors ("coopetitors").

This is especially true since the U.S. technology sector is highly dynamic and flexible, whereas the Tech War itself doesn't support American innovation capacity (Gewirtz, 2019; Manuel and Hicks, 2020; Goodrich and Su, 2020). What is even worse, the Tech War may result in what the U.S. tries to prevent – i.e., rise of China as a global center of advanced electronics and digital innovation. Chinese "smart response" (investments in human capital, R&D, etc.) to the U.S. sanctions is already beefing up Chinese innovation, technological, and manufacturing capacities. And full technology blockade was always a

very problematic issue, while evading sanctions is rather a technical issue (also through informal import of competences like in case of P.R.C.'s «buying out» Taiwanese experts in microelectronics (Cheng, 2020)).

However, the problem is that the Tech War is not – and never was – purely economic phenomenon, but a highly securitized aspect of a new "Great Game" of the superpowers.

Casus Belli

The U.S. post-Cold War restrictions on trade and cooperation with the P.R.C. in different dual-use or strategic high-tech areas like aerospace were always present (Petland, 2011; Nelson, 2014). For the ICT a change in mode of bilateral relationships occurred since early 2010s. Several major reasons pushed the United States to a harder course toward China.

First of all, 2010s witnessed sharp rise of Chinese manufacturing and innovation capacity. The best illustration of changes that occurred was the rise of Huawei empire. The company developed competitive telecommunication equipment (including viable 5G standards), advanced Kirin chip design, and globally recognizable smartphone brand. P.R.C. digital prowess revealed itself also in booming patenting and publication activities in different areas related to the emerging technologies like AI (WIPO, 2019; Savage, 2020; Correia and Reyes, 2020).

A closely related factor was P.R.C. ambitious policies for digital development. As many other catching-up nations, Chinese elites accented so-called developmental state practices with strong neo-techno nationalist accents (Ostry and Nelson, 1995; Nakayama, 2012; Wade, 2018; Manning, 2019; Capri, 2020). Correlated with import substitution macro-strategy, neo-techno nationalism exploits specific conditions of the economic globalization (intensified FDI, trade, etc.) for strengthening national technological sovereignty in areas considered to be critical for long-term sustained economic growth and security. Among other instruments, this neo-techno nationalist/developmental focus resulted in the extensive use of practices considered by the Western nations as unfair (forced technology transfer in what may be called as "compulsory offset deals"; guarding some national "strategic" markets – including the Internet ones, excessive state support and protectionism, and more). The ICT as critically important sector was at the center of these efforts – with electronic industry and national telecomm standards among most known examples (Shim and Dong, 2016; Lee and Kwak, 2020; Capri, 2020). With time archaic XX-century-styled industrial policy instruments were supplemented with

advanced measures to support human capital, venture ecosystems, science parks, and other important elements of national innovation systems. Still, even then excessive public interventions were the case – from restrictions on foreign investments and up to different preferences to the state-owned enterprises or privately-owned "national champions". For many years sales on the fast-growing Chinese market were seen as an adequate compensation for these risks, while P.R.C. tech challenge was not seen as critical. But rise of the science and technology power and new ambitious goals of the Chinese leadership in 2010s changed minds of the Western decision makers. And especially it was true for the U.S.A. that anticipated rivalry between the two superpowers. As a trigger of change, one may mention "Made in China 2025" program adopted in 2015. The initiative was condemned by many American politicians and part of the expert community, and provoked some concerns on the U.S. business side. "Made in China 2025" even became part of the American agenda on negotiations to settle the U.S.-China trade dispute in 2019 (U.S. Chamber of Commerce, 2017; Laskai, 2018; U.S. Congress, 2019; Cafruny, 2019; Wei, 2019; Davis and Wei, 2019; Cory and Atkinson, 2020; Ding and Dafoe, 2021).

Another issue – also related to a proactive P.R.C. economic policy – was Chinese investment expansion on the Western markets, especially since 2008-2009 crisis. Among other assets, in focus were American and European established technology companies, including global leaders like American Broadcom Inc. or German Kuka Roboter. And it is important to mention that at least some of these strategic assets were targeted by the Chinese state-owned or state-related enterprises (CFIUS Scoreboard, 2018). In search for new business ideas, technologies, and "entry tickets" to the Western markets Chinese entities intensified investments in the U.S. venture sector – especially since 2015, with peak in 2017 (more than 400 deals and about $6.5bln invested) (Gonzales and Ohara, 2018; Ruehl et al., 2019). Despite the reason for this investment "invasion" were economic (also considering developmental logic), its possible strategic consequences challenged U.S. interests (Bradsher and Mozur. 2016; Bellinger et al., 2016).

Finally, traditional hard power and strategic considerations play a role. Here special concern of the U.S.A. was P.R.C. technology transfer from the civilian to the military sector, reformulated by Xi Jinping in a so-called Civilian-Military Fusion strategy (Besha, 2011; Lafferty, 2019; Bitzinger, 2021; Kania and Laskai, 2021). The new policy was neither totally unexpected, nor all-embracing or super effective. More than all, it was not something unseen, since Beijing simply tried to make a Chinese version of well-established U.S. practices of tech dialogue and cooperation between defense and civilian sectors. But

in a general context of bilateral relationship, it strengthened American suspicions against China, its digital companies, and became (at least officially) an important factor for the Tech War (Manuel and Hicks, 2020; U.S. Department of Defense, 2020).

Unsurprisingly, since the beginning of 2010s political elites in Washington, as well as defense and intelligence community paid more attention to the Chinese "Digital Challenge" outside of traditional dual-use and defense technologies. For example, in October 2012 the U.S. House Permanent Select Committee on Intelligence started investigation on potential security risks of Huawei and ZTE technologies.

But most visibly this new trend revealed itself in the evolution of activities of the Committee on Foreign Investment in the United States (CFIUS) (Bellinger et al. 2016; Bradsher and Mozur. 2016; CFIUS Scoreboard, 2018). During 2010s up to 16-20% of all CFIUS reviews were allegedly related to the Chinese acquisitions – with rising number of high-tech cases. Number of ICT-related deals abandoned because of the CFIUS position also rose since 2015-2016. Among most known were failed bids of Tsinghua Unigroup for Micron and for 15% stake of Western Digital, and GO Scale Capital for Lumileds. However, until the end of 2016 CFIUS mostly applied "soft" approach. It didn't overreacted and was able to stop unwanted deals just by signaling its position to the sides (e.g., communicating concerns or hinting on "expected" prohibition of a deal). Situation changed in December 2016. CFIUS recommended to reject, and President Barack Obama prohibited acquisition of the U.S. business of German Aixtron SE (semiconductor equipment manufacturer, also an important supplier for the U.S. military aerospace) by Fujian Grand Chip Investment, blocking the whole deal (Bellinger et al., 2016). It seemed to be a kind of landmark or symbolic decision indicating the changes occurred, especially since it was only third time in two decades when U.S. Government blocked Chinese acquisition.[3]

The winds changed in other areas too, revealing new U.S. technology containment policy – absent in high-level documents like National Security Strategies, but felt in de-facto agendas of key federal agencies and U.S. Congress (like Wolf Amendment, cutting NASA's cooperation with China since FY2012). It was also in line with general U.S. trade and investment policies clearly focused at reduction of China's economic and strategic influence, from the U.S.-India dialogue and up to negotiations on Transatlantic

[3] First one was in 1990 (bid for specialized aircraft parts producer MAMCO Manufacturing Inc.by state-owned CATIC), and the second in 2012 (construction of a wind farm near the U.S. Navy base by Ralls Corp.)

Trade and Investment (TTIP) and Trans-Pacific (TAP) Partnerships.[4]

So, when Donald Trump, a long-standing critic of Chinese policies, entered the White House, the stage for the technology war was already settled. Still, it was Trump who shaped the Tech War – presumably, also because he was less associated with the traditional political elites and thus not so constrained with established practices or international political "etiquette".

Political Economy of The Tech War: First Modern Conflict?

Political economy of the Tech War may be conceptualized using existing body of knowledge about sanctioning policy (see, for example: Kaempfer and Lowenberg, 2007; Hufbauer et al., 2008). There were at least three blocks of rationales and goals, reflecting both traditional practices – always present in the economic confrontation of superpowers, as well as the post-Cold War realities.

First of all, there are rationales and efforts that may be labelled as "realist". Following M. Mastanduno's framework, we may identify it as a combination of a "strategic embargo" (halting exports of defense or critical dual-use technologies) and "economic war" (restrictions on the transfer of technologies important for long-term rise of adversary's total capacity) (Mastanduno, 1985). From a formal point of view, a separate block of rationales is presented by the cyber-security challenges, a specific XXI-century concern. But it is still very "realist" in nature since it is linked to the hard power issues.

Second block relates to the values and human rights. Here we may find "punishment" and denouncements for alleged digital oppression against Uyghur minorities, as well as for general efforts to build Chinese Surveillance State (Barnes, 2021; Chan, 2021; CNBC, 2021). In both cases the rationales may be linked either to the Post-Cold War value-based policy concept, or with established "moral opposition to the repressions", that existed in the U.S. policies for decades (e.g., American sanctions for the U.S.S.R.'s Jewish immigration policies). It is worth noting that in Chinese own views this block is also seen as "realist", just disguising the "economic war" efforts.

Finally, there was a competitiveness rationale, mostly focused on stopping P.R.C. "unfair" trade and investment practices. Almost invisible in official statements and documents, as well as in the actual sanctions, it was and still is real and important. Once

---

[4] See, for example Barack Obama's statement on Pacific trade agreement in his 2015 State of the Union Address: China wants to write the rules for the world's fastest-growing region. That would put our workers and our businesses at a disadvantage. Why would we let that happen? We should write those rules" (Obama, 2015).

again, depending on the point of view associated measures may be interpreted either as supporting "level playing field" on Chinese and global markets, or as preventing further rise of the Chinese tech companies - as competitors for the American ones and source of financial and digital power to the P.R.C.

Most of these goals and rationales look very familiar. On one hand, we may see clear similarities between the Tech War and the Cold War – mostly because in both cases we may see confrontation between the superpowers and capacity-affecting measures. The economic war also gains some resemblance with other geopolitical conflicts of the last decades, including U.S. policies on Iran, North Korea, and Post-Crimea Russia. On the other hand, some clear parallels may be also drawn between the 2018-2021 situation and the U.S.-Japan conflict over semiconductor and electronics markets in late 1970s - early 1990s.

However, a more detailed analysis reveals that in reality the Tech War has rather eclectic nature with notable difference between these two structural conflicts of the XX century.

U.S.S.R. never considered commercial high-tech markets in general – and civilian digital technologies in particular – as factor enhancing its power or an important source of revenue for development. Despite there were attempts to rise Soviet commercial high-tech export to the West,[5] it never was top priority and had almost zero economic consequences. In its foreign economic policy, also in high-tech area, U.S.S.R. accented rather formation of an "alternative" trade and financial/investment system (See, for example, brilliant economic history compendium: (Khanin, 2008)). This situation was explained by both geopolitical and economic reasons. Any normal trade and investment relationships between the U.S.S.R. and capitalist economies during the Cold War were unrealistic. So was the scalable Soviet commercial high-tech exports and competition with the West. Soviet commercial high-tech sector was chronically underinvested and lacked dynamism due to the specifics of the socialistic economy and economic ideology accenting industrial supply (so-called "A-category goods") and defense sector. The only areas of the science and technology competition with the West were politically symbolic dual-use areas like space or high-energy physics with very small or none commercial potential.

On the contrary, Japan accented commercial sector. Since at least the middle of 1980s

[5] Sony's co-founder and Chairman Akio Morita was even asked to advise Soviet top industrial officials how to commercialize small TV sets on the capitalistic markets (Morita, 2014).

some experts and politicians speculated about possible role of Japanese digital and other high-tech prowess as factor of defense and security capacity and geopolitical influence (Vogel, 1989; Ishihara, 1991). But even the possibility of this power transmutation was challenging. And it is still questionable whether Japan in this period could and want to (considering its own national interests and available resources) reinstate its role in the global politics and international relations – not even saying about challenging U.S. hegemony. Interesting, but it seems that power and security implications of the semiconductor conflict were seen mostly on the American, not Japanese side. Part of the defense community interpreted possible U.S. dependence on the imported strategic electronic components as a risk in case of war, while different elite groups considered broader competitiveness issues as a challenge to the U.S. hegemony.[6]

Neo-techno nationalist challenge of China intertwined with rise of its regional and global strategic role looks different from both the U.S.S.R. and Japanese cases. So is the U.S. Tech War countermeasures that are neither CoCom[7]-styled technology sanctions, nor the analogue of the 1980s semiconductor conflict with Japan.

This eclectic nature of the Tech War is not accidental but reveals changes in global politics and economy induced by the digital transformation and reactions of the elites on this new realm.

In a world with growing importance of the high-tech sectors in global GDP, trade, and development, emerging and advanced technologies proved to be not only key source of competitiveness, but also a factor of building power architectures. Outside of defense/security issues and capacity building this also relates to the control over critical technologies and GVC elements as factor influencing capacity development of the third parties (as in case of halting ASML's EUV export to China). The market dominance affects (re)construction of power and leadership too: amid profits it also provides preferential access to the talents and raw data as critical competitiveness factors in the digital economy.

Despite most of these phenomena aren't new, in the realm of digitalizing economy they gain more importance – economic and (geo)political. In the latter case what makes difference is raising securitization and weaponization of digital (especially emerging)

---

[6] Both these ideologies were reflected in the emergence of the SEMATECH consortia supported by the federal authorities in response to the Japanese semiconductor "invasion" " (see, for example: Charles, 1988).

[7] Coordinating Committee for Multilateral Export Controls. On history and basic activities of the CoCom see: (Office of Technology Assessment, 1979: 153-179).

technologies. Despite new technology developments – critical or other "game-changing" – were always securitized, in 2010s this process was reinforced by several factors. One was hype-styled "technology revolution" narratives – from the Industry 4.0 and up to speculations on the AI (Anton et al., 2006; Brynjolfsson and McAfee, 2016; Rifkin, 2014; Schwab, 2017). The other was the return of trade/investment conflicts and revised protectionism from a forgotten past of 1980s to perilous present and nascent future of the international relations– presumably, a consequence of imperfect national reactions on rising global competition (Evenett, 2019). Finally, there were some specific political and economic challenges, like American fears of losing markets and employment to the developing nations, or Chinese ideology of "catching up and surpass [the West]" ("ganchao") (Atkinson and Ezell, 2012; Gewirtz, 2019).

This tandem of traditional securitization and "revolutionary" concepts enhanced by other economic factors explains also the Tech War as a specific form of innovation conflict between the two superpowers. Both sides obviously see it as a zero-sum game rather than coopetition,[8] since future and global leadership are not tradable.

As a result, digital technologies and global markets are more and more interpreted not only as strategic resources for capacity formation or competitiveness, but also as factors of institutional and structural power[9] (Ding and Defoe, 2021). Here we may see almost H. Mackinder's ideology for the digital era ("who controls [digital technology] x, controls the world"). It is well illustrated by the confrontation over 5G, microelectronics, AI – and by efforts to localize "critical" tech infrastructure in both China and the U.S.A. as factor of "control" and tech sovereignty (see, for example, on the U.S. efforts: (Clark and Swanson, 2020; Rampton, 2020; The White House, 2022)). Not less important, this vision is shared by elite groups in other parts of the world. One can remember Russian President Vladimir Putin's speech in 2017, full of veiled criticism of the U.S. digital "monopolistic" ambitions, where he stated: "The one who will become a leader in this [AI] area will be the master of the world" (RIA Novosti, 2012). Alike sentiments are also felt in the E.U. – especially in European digital sovereignty concepts (for E.U. concepts see: (European Union, 2019; Hobbs, 2020; Komaitis and Sherman, 2021)).

This complex political economy of the Tech War, in turn, presumably represent new

---

[8] Cooperation and competition among companies – see on the state of research on this phenomenon (Gernsheimer et al., 2021).

[9] A de-facto interpretation of digital tech as a form of structural and institutional power may be seen in the discussions on 5G. On classification and characteristics of different forms of power see (Barnett and Duvall, 2005).

step in *marketization* of geopolitics in the knowledgeable global economy. Amid growing importance of technological issues, we see how traditional *technological restrictionism* of the strategic embargoes and economic wars of the past is slowly evolving into the *innovation expansionism* (factor of market/innovation dominance and structural power). Setting aside regional technology blocks, data colonialism, and other possible outcomes, in a very dialectic manner this outward-oriented ideology also presupposes strong neo-techno nationalist sentiments as factor defending national technology sovereignty. And despite Russia-West confrontation may for some time reverse these transformations toward more traditional geopolitical strategies, it seems that the future of geopolitics will be much more intertwined with the digital technologies and generally high-tech. Considering its dynamism, role in GVCs, and renewed technology competitiveness, Asia will be at the heart of these new processes: as an epicenter of digital transformation, battleground in this new Great Game, and "living lab" or trend-setter of techno-geopolitics. This forms new challenges and risks for Japan and other Asian nations – but new opportunities as well.

References:

Anton, P.S., Silberglitt R. & Howell D.R. et al. (2006). *The Global Technology Revolution 2020, In-Depth Analyses. Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications.* RAND Corporation, Document # MR-1307-NIC. Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR303.pdf [Accessed: Nov. 1, 2021].

Atkinson, R.D. and Ezell, S.J. (2012). *Innovation Economics: The Race for Global Advantage.* New Haven, Yale University Press.

Barefoot K., Curtis D., Jolliff W., Nicholson J.R., Omohundro R. (2018). Defining and Measuring the Digital Economy. Working Paper, *The Bureau of Economic Analysis*, U.S. Department of Commerce. Available at: https://www.bea.gov/system/files/papers/WP2018-4.pdf [Accessed: Nov.14, 2021].

Barkin, N. (2020). Export controls and the US-China tech war. *MERICS China Monitor.* Available at: https://merics.org/en/report/export-controls-and-us-china-tech-war [Accessed: Oct.10, 2021].

Barnes J.E. (2021). U.S. Cracks Down on Firms Said to Aid China's Repression of Minorities. *The New York Times,* Dec. 16. Available at: https://www.nytimes.com/2021/12/16/us/politics/us-china-biotech-muslim-minorities.html [Accessed: Dec.21, 2021].

Barnett, M., & Duvall, R. (2005). Power in international politics. *International organization,* 59(1): 39-75. DOI: 10+10170S0020818305050010.

Bellinger III, J.B., Barker J.P., Blanchard C.A., Lee R.D., Reade C.E., Perkins N.L., Townsend N.L., McSorley T. (2016). Presidential Prohibition of Chinese Company Purchase of Semiconductor Firm Highlights Increased U.S. Government Scrutiny of Chinese Investments. *Arnold & Porter,* Dec. 21. Available at: https://www.arnoldporter.com/en/perspectives/publications/2016/12/presidential-prohibition-of-chinese [Accessed: Dec.21, 2021].

Besha, P. (2011) Civil-Military Integration in China: A Techno-Nationalist Approach to Development. *American Journal of Chinese Studies*, 18(2): 97-111.

Bitzinger, R.A. (2021). China's Shift from Civil-Military Integration to Military-Civil Fusion. *Asia Policy*, 16 (1): 5-24. DOI: 10.1353/asp.2021.0001.

Bradsher K., Mozur P. (2016) Political Backlash Grows in Washington to Chinese Takeovers. *The New York Times,* Feb. 16. Available at: https://www.nytimes.com/2016/02/18/business/dealbook/china-fairchild-semiconductor-bid-rejected.html [Accessed: Oct.20, 2021].

Bresnahan, T. (2010). General purpose technologies. In: *Handbooks in Economics*. Vol.2. / Hall B.H., Rosenberg N. (Eds.). North Holland: Elsevier. P. 761-791.

Brynjolfsson, E., McAfee, A. (2016). *The Second Machine Age.* N.Y.: W. W. Norton&Company.

Cafruny, A. W. (2019). Can the United States Contain China? *Russia In Global Affairs*, 17 (1): 100-122. DOI: 10.31278/1810-6374-2019-17-1-100-122.

Capri, A. (2020). Techno-nationalism: The US-China Tech Innovation Race. New Challenges for Markets, Business and Academia. *Hinrich Foundation Report.* Available at: https://research.hinrichfoundation.com/hubfs/White%20Paper%20PDFs/US-China%20innovation%20race%20(Alex%20Capri)/Hinrich%20Foundation%20-%20Techno-nationalism%20and%20the%20US-China%20tech%20innovation%20race%20-%20Alex%20Capri%20-%20August%202020.pdf [Accessed: Sept.15, 2021].

CFIUS Scoreboard (2018). *U.S.-China Transactions Jan.2014-September 2018.* Pillsbury Winthrop Shaw Pittman LLP. Available at: https://www.pillsburylaw.com/images/content/1/1/119897.pdf [Accessed: Oct.1, 2021].

Chan V. (2021) U.S. to Add SenseTime to Investment Blacklist Ahead of IPO. *Bloomberg,* Dec.9. Available at: https://www.bloomberg.com/news/articles/2021-12-09/u-s-to-blacklist-sensetime-ahead-of-hong-kong-ipo-ft-reports [Accessed: Dec.11, 2021].

Chang, G.G. (2020). *The Great U.S.-China Tech War*. Encounter Books.

Charles D. (1988). Reformers Seek Broader Military Role in Economy. *Science*, 241 (4867): pp. 779-781. DOI: 10.1126/science.241.4867.779.

Cheng, T.-F. (2020). China Hires over 100 TSMC Engineers in Push for Chip Leadership, *Nikkei Asian Review,* August, 12. Available at: https://asia.nikkei.com/Business/China-tech/China-hires-over-100-TSMCengineers-in-push-for-chip-leadership [Accessed: Sept.13, 2022]

Clark, D., Swanson, A. (2020). T.S.M.C. Is Set to Build a U.S. Chip Facility, a Win for Trump. *The New York Times,* May 14. Available at: https://www.nytimes.com/2020/05/14/technology/trump-tsmc-us-chip-facility.html [Accessed: Sept. 18, 2021].

Correia, A., Reyes, I. (2020). *AI research and innovation: Europe paving its own way.* European Commission, R&I Paper Series, Working Paper 2020/15. Luxembourg: Publications Office of the European Union. DOI: 10.2777/264689.

CNBC (2021). U.S. adds 14 Chinese companies, to economic blacklist over Xinjiang. *CNBC,* Jul 10. Available at: https://www.cnbc.com/2021/07/10/us-adds-14-chinese-companies-to-economic-black-list-over-xinjiang.html [Accessed: Oct.16, 2021].

Cory, N., Atkinson, R.D. (2020). Why and How to Mount a Strong, Trilateral Response to China's Innovation Mercantilism. *Information Technology & Innovation Foundation*. Available at: itif.org/sites/default/files/2020-trilateral-china.pdf [Accessed: July 30, 2021].

Danilin, I.V. (2021). The U.S.-China Technological War: Digital Technologies as a New Factor of World Politics? *Russia in Global Affairs*, 19 (4): 78-96. DOI: 10.31278/1810-6374-2021-19-4-78-96.

Davis, B., Wei, L. (2019). China's Plan for Tech Dominance Is Advancing, Business Groups Say. *The Wall Street Journal,* Jan. 22. Available at: https://www.wsj.com/articles/u-s-business-groups-weigh-in-on-chinas-technology-push-11548153001 [Accessed: Sept. 30, 2021].

Ding, J., Dafoe, A. (2021). The Logic of Strategic Assets: From Oil to AI. *Security Studies*, 30(2): 182-212. DOI: 10.1080/09636412.2021.1915583.

European Union (2019). Expanding the EU 's Digital Sovereignty. *Official website of Germany's Presidency of the Council of the European Union*, 27 October. Available at: www.eu2020.de/eu2020-en/eu-digitalisation-technologysovereignty/2352828 [Accessed: July 30, 2021].

Evenett, S., J. (2019). Protectionism, State Discrimination, and International Business since the Onset of the Global Financial Crisis. *Journal of International Business Policy,* 2(1): 9–36. DOI:10.1057/s42214-019-00021-0.

Gernsheimer, O., Kanbach, D.K., Gast, J. (2021). Coopetition research - A systematic literature review on recent accomplishments and trajectories. *Industrial Marketing Management*, 96:113-134. DOI: 10.1016/j.indmarman.2021.05.001.

Gewirtz, J.B. (2019). China's Long March to Technological Supremacy. *Foreign Affairs*, 27 August. Available at: www.foreignaffairs.com/articles/china/2019-08-27/chinas-long-march-technological-supremacy [Accessed: July 30, 2021].

Gonzales, J., Ohara, F. (2019). Chinese venture investments in the United States, 2010–2017. *Thunderbird International Business Review,* 61 (2): 123-131. DOI: 10.1002/tie.22017.

Goodrich J., Su Z. (2020). The U.S. Should be Concerned with its Declining Share of Chip Manufacturing, Not the Tiny Fraction of U.S. Chips Made in China. *Semiconductor Industry Association,* July 10. Available at: https://www.semiconductors.org/the-largest-share-of-u-s-industry-fab-capacity-is-in-the-united-states-not-china-lets-keep-it-that-way/ [Accessed: Aug. 1, 2021].

Grimes, S., Du, D. (2022). China's emerging role in the global semiconductor value chain. *Telecommunications Policy*, 46 (2). DOI: 10.1016/j.telpol.2020.101959.

Hobbs, C. (ed.) (2020). Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of U.S.-China Rivalry. *The European Council on Foreign Relations*. Available at: www.ecfr.eu/page/-/europe_ digital_sovereignty_rulemaker_superpower_ age_us_china_rivalry.pdf [Accessed: July 30, 2021].

Hufbauer, C.G., Schott, J., Elliott, K.A. and Oegg, B. (2008). *Economic Sanctions Reconsidered*. 3rd Edition. Washington, DC: Peterson Institute for International Economics.

IC Insights (2021) China Forecast to Fall Far Short of its "Made in China 2025" Goals for ICs. *IC Insights Research Bulletin,* Jan. 06. Available at: https://www.icinsights.com/data/articles/documents/1330.pdf [Accessed: July 30, 2021].

International Monetary Fund (2018). Measuring The Digital Economy. *The IMF Staff Report*. Available at: https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy [Accessed: Dec.12, 2021].

Ishihara, S. (1991). *The Japan That Can Say No: Why Japan Will Be First Among Equals.* New York: Simon & Schuster.

Jovanovic, B., Rousseau, P.L. (2005). General purpose technologies. In: *Handbook of Economic Growth*, Vol. 1B / Aghion, P., Durlauf, S.N. (Eds.). Elsevier B.V. P. 1181-1224.

Kaempfer, W.H., Lowenberg, A.D. (2007). The Political Economy of Economic Sanctions. In: *Handbook of Defense Economics*, Vol. 2. / T. Sandler and K. Hartley (eds.).

Amsterdam: Elsevier, pp. 867-911. DOI: 10.1016/S1574-0013(06)02027-8.

Kania, E.B., Laskai, L. (2021). Myths and Realities of China's Military-Civil Fusion Strategy, *Center for a New American Security*. Available at: https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy [Accessed: Nov. 11, 2021].

Khanin, G.I. (2008). *Ekonomicheskaya istoriya Rossii v noveishee vremya* [Economic History of Russia in Modern Times], Vol. 1. Novosibirsk: Novosibirsk State Technical University. (In Russ.).

Komaitis, K., Sherman, J. (2021). US and EU tech strategy aren't as aligned as you think. *The Brookings Institution.* Available at: https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/ [Accessed: Oct.30, 2021].

KPMG (2021) Venture Pulse Q4. *KPMG Private Enterprise.* Available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/01/venture-pulse-q4-2020-report-asia.pdf [Accessed: Nov.12, 2021].

Lafferty, B. (2019). Civil-Military Integration and PLA Reforms. In: *Chairman Xi Remakes the PLA* / Phillip C. Saunders, Arthur S. Ding, Andrew Scobell, Andrew N.D. Yang, and Joel Wuthnow (Eds.). National Defense University Press. Pp.: 627-660. Available at: https://ndupress.ndu.edu/Portals/68/Documents/Books/Chairman-Xi/Chairman-Xi.pdf [Accessed: Nov. 5, 2021].

Laskai, L. (2018). Why Does Everyone Hate Made in China 2025? *Council on Foreign Relations,* March 28. Available at: https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025 [Accessed: Nov.10, 2021].

Lee, H.; Kwak, J. (2020). The Changing Patterns of China's International Standardization in ICT under Techno-nationalism: A Reflection through 5G Standardization. *International Journal of Information Management*, 54. DOI: 10.1016/j.ijinfomgt.2020.102145.

Manning, R. (2019). Techno-Nationalism vs. the Fourth Industrial Revolution. *Global Asia,* 14(1). Available at: https://www.globalasia.org/v14no1/cover/techno-nationalism-vs-the-fourthindustrial-revolution_robert-a-manning [Accessed: July 7, 2021].

Manuel, A., Hicks, K. (2020). Can China's Military Win the Tech War? *Foreign Affairs*, 29 July [online]. Available at: https://www.foreignaffairs.com/articles/united-states/2020-07-29/can-chinas-military-win-tech-war [Accessed: Aug. 7, 2021].

Mastanduno, M. (1985). Strategies of Economic Containment: U.S. Trade Relations with the Soviet Union. *World Politics*, 37(4): 503-531.

Morita, A., Reingold, E.M., Shimomura, M. (1986). *Made in Japan.* N.Y.: E. P. Dutton

Nakayama, S. (2012). Techno-Nationalism versus Techno-Globalism. *East Asian Science,*

Technology and Society, 6 (1): 9–15. DOI: 10.1215/18752160-1504708.
National Science Board (2020). *The State of U.S. Science and Engineering 2020. Science & Engineering Indicators*. NSB-2020-1. Alexandria, VA.
National Venture Capital Association (2021). *NVCA Yearbook 2021*. Available at:https://nvca.org/wp-content/uploads/2021/08/NVCA-2021-Yearbook.pdf [Accessed: Nov.01, 2021].
Nelson, C. (2014). U.S. Space Industry Deep Dive Assessment: Impact of U.S. Export Controls on the Space Industrial Base. *U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation.* Technical Report. DOI: 10.13140/RG.2.2.16632.47368.
Obama, B. (2015). *Remarks by the President in State of the Union Address.* January 20, 2015. U.S. Capitol. Washington, D.C. https://obamawhitehouse.archives.gov/the-press-office/2015/01/20/remarks-president-state-union-address-January-20-2015 [Accessed: Oct.27, 2021].
OECD (2020). *OECD Digital Economy Outlook 2020.* Paris: OECD Publishing. DOI: 10.1787/bb167041-en.
Office of Technology Assessment (1979). *Technology and East-West Trade.* OTA Report. NTIS order #PB83-234955. Washington, D.C.: U.S. Government Printing Office.
Ostry, S., Nelson, R.R. (1995). *Technonationalism and techno-globalism.* Wash., D.C.: The Brookings Institution.
Petland, W. (2011). Congress Bans Scientific Collaboration with China, Cites High Espionage Risks. *Forbes,* May 7. Available at: https://www.forbes.com/sites/williampentland/2011/05/07/congress-bans-scientific-collaboration-with-china-cites-high-espionage-risks/?sh=1c83934d4562 [Accessed: Nov. 25, 2021].
Pitchbook (2020). *European Venture Report. 2020 Annual Report*. Available at: https://files.pitchbook.com/website/files/pdf/2020_Annual_European_Venture_Report.pdf [Accessed: Oct.25, 2021].
Rampton, R. (2020). Trump Gives Medical Stockpile A 'Kodak Moment' With New Loan To Make Drugs. *NPR*, July 28. Available at: https://www.npr.org/sections/coronavirus-live-updates/2020/07/28/896209016/trump-gives-medical-stockpile-a-kodak-moment-with-new-loan-to-make-drugs [Accessed: Aug.25, 2021].
RIA Novosti (2017). Putin: lider v sfere iskusstvennogo intellekta stanet vlastelinom mira [Putin: the leader in the field of artificial intelligence will become the master of the world]", *RIA Novosti,* September 1, Available at: https://ria.ru/20170901/1501566046.html [Accessed: Nov.25, 2021]. [In Russ.]

Rifkin, J. (2014). *Zero Marginal Cost Society.* New York, Palgrave MacMillan.

Rogers M., Dutch C.A. (2012). Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. *U.S. House of Representatives.* 112th Congress. Available at: accessed:https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf [Accessed: Sept.15, 2021].

Ruehl, M., Kynge, J., and Kruppa, M. (2019). Chinese venture capital investment in US falls to four year low. *Financial Times,* October 2. Available at: https://www.ft.com/content/440fecb8-e4cd11e9-b112-9624ec9edc59 [Accessed: Aug.25, 2021].

Savage N. (2020). Learning the algorithms of power. *Nature,* 588 (Supplement): S102-S104. DOI: 10.1038/d41586-020-03409-8.

Schwab, K., 2017. *The fourth industrial revolution.* New York, Currency Books.

Semiconductor Industry Association (2020). *State Of The U.S. Semiconductor Industry*. Available at: www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf [Accessed: Sept. 30, 2021].

Shim, Y., Dong, H. S. (2016). Neo-Techno Nationalism: The Case of China's Handset Industry. *Telecommunications Policy,* 40 (2–3): 197–209. DOI: 10.1016/j.telpol.2015.09.006.

Sun, H., 2019. U.S.-China Tech War: Impacts and Prospects. *China Quarterly of International Strategic Studies*, 5(2): 197–212. DOI: 10.1142/S237774001950012X.

The White House (2022). *Biden-Harris Administration Bringing Semiconductor Manufacturing Back to America*. Fact Sheet, Jan.21, Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-bringing-semiconductor-manufacturing-back-to-america-2/ [Accessed: Sept.19, 2021].

The World Bank (2021). *ICT goods exports (% of total goods exports).* Available at: https://data.worldbank.org/indicator/TX.VAL.ICTG.ZS.UN [Accessed: Aug.3, 2021].

Thomas C.A. (2021). Lagging But Motivated: The State of China's Semiconductor Industry. *Brookings Institution,* January 7. Available at: https://www.brookings.edu/techstream/lagging-but-motivated-the-state-of-chinas-semiconductor-industry/ [Accessed: Aug.3, 2021].

U.S. Chamber of Commerce (2017). *Made in China 2025: Global Ambitions Built on Local Protections.* Available at: https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf [Accessed: Sept.10, 2021].

U.S. Congress (2019) *Made in China 2025 and the Future of American Industry*. U.S.

Congress. Hearing before the Senate Small Business and Entrepreneurship Committee. February 27, 2019. Available at: https://www.sbc.senate.gov/public/index.cfm/2019/2/made-in-china-2025-and-the-future-of-american-industry [Accessed: Oct.10, 2021].

U.S. Department of Defense (2020). *Military and Security Developments Involving the People's Republic of China 2020.* Annual Report to Congress. Available at: media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DODChina-military-power-report-final.pdf [Accessed: Oct. 30, 2021].

UNCTAD (2019). *Digital Economy Report 2019.* New York, United Nations Publications. Available at: https://unctad.org/system/files/official-document/der2019_en.pdf [Accessed: Aug.1, 2021].

Vogel, S.K. (1989). Japanese High Technology, Politics, and Power. Berkeley. *Roundtable on the International Economy.* Research Paper #2. University of California, Berkeley. Available at: ageconsearch.umn.edu/record/292939/files/ucb-0002.PDF [Accessed: July 30, 2021].

Wade, R.H. (2018). The Developmental State: Dead or Alive? *Development and Change*, 49 (2): 518–546. DOI: 10.1111/dech.12381.

Wei, L. (2019). Beijing Drops Contentious 'Made in China 2025' Slogan, but Policy Remains. *The Wall Street Journal,* March 5. Available at: https://www.wsj.com/articles/china-drops-a-policy-the-u-s-dislikes-at-least-in-name-11551795370 [Accessed: Aug. 12, 2021].

WIPO (2019). *WIPO Technology Trends 2019. Artificial Intelligence.* World Intellectual Property Organization. Geneva: WIPO. 154 p. Available at: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf [Accessed: Aug. 18, 2020].

Xi, C. (2021) Chip Wars And Decoupling: China And The US's Semiconductor Plays. *AsiaGlobal Online (AGO)*, June 3. Available at: https://www.asiaglobalonline.hku.hk/chip-wars-and-decoupling-china-and-uss-semiconductor-plays [Accessed: Aug. 21, 2021].

Zhao, J. (2021). The Political Economy of the U.S.-China Technology War. *Monthly Review,* 73 (3). Available at: https://monthlyreview.org/2021/07/01/the-political-economy-of-the-u-s-china-technology-war/ [Accessed: Oct. 22, 2021].

Contributors (as of December 2021)

Mr. Bryan Clark is a senior fellow and Director of the Center for Defense Concepts and Technology at Hudson Institute. He leads studies there in naval operations and fleet architecture, electronic warfare, autonomous systems, military competitions, 5G telecommunications, and command and control. Before joining Hudson Institute, Bryan was a senior fellow at the Center for Strategic and Budgetary Assessments (CSBA), where he led studies for the DoD Office of Net Assessment, Office of the Secretary of Defense, and Defense Advanced Research Projects Agency on new technologies and the future of warfare. Prior to joining CSBA, he was special assistant to the Chief of Naval Operations and director of his Commander's Action Group, where he led development of Navy strategy and implemented new initiatives in electromagnetic spectrum operations, undersea warfare, expeditionary operations, and personnel and readiness management. During his 25-year Navy career, Bryan was an enlisted and officer submariner, serving in afloat and ashore submarine operational and training assignments including tours as chief engineer of two nuclear submarines and operations officer at the Navy's nuclear power training unit. He has a Master of Science degree in national security studies from the U.S. National War College, a Bachelor of Science degree in chemistry and philosophy from the University of Idaho and conducted graduate research in chemistry at the University of Washington. .

Dr. Fujita Motonobu is a policy coordinator of the technology policy office at the Acquisition Technology and Logistics Agency (ATLA), MOD. He specializes in mid-to-long term planning on applied researches for defense equipment and technology strategy on defense science. His recent work was to draft "R&D vision toward realization of Multi-Domain Defense Force and Beyond," which was published by MOD in August 2019. Prior to his current assignment, as the chief technology strategist, he drafted the R&D vision at the planning office of ATLA. From 2013 to 2017, he led an applied research project on high-power microwave systems. From 2011 to 2013, as a research scientist of Department of Guided Weapon Systems Development, Technical Research and Development Institute (TRDI), he worked as a project team member of SM-3 Block IIA Cooperative Development (SCD) project. He supported project management activities on the development of missile components. His first carrier in MOD was a research scientist. He was involved in applied research and ground tests on missile components such as warheads and radio-proximity fuzes and safety devices under development from 2006 to 2011. His doctorate is in Information Physics and Computing from the

University of Tokyo, where he wrote a thesis on power-performance optimization on microprocessors with software-controlled on-chip memories.

Dr. Tai Ming Cheung is director of the Institute on Global Conflict and Cooperation <http://igcc.ucsd.edu/> at the University of California, San Diego in La Jolla. Among the areas of his research focus include China's efforts to become a world-class science and technology power, and the relationship between geo-economics, innovation, and national security. Dr. Cheung is also a professor at the School of Global Policy and Strategy at UC San Diego. Dr. Cheung is a long-time analyst of Chinese and East Asian defense and national security affairs, especially defense economic, industrial and science and technological issues. He is the author of Fortifying China: The Struggle to Build a Modern Defense Economy (Cornell University Press, 2009), editor of Forging China's Military Might: A New Framework for Assessing Innovation (Johns Hopkins University Press, 2014), co-editor of The Gathering Pacific Storm: Emerging US-China Strategic Competition in Defense Technological and Industrial Development (Cambria Press, 2018), and author of Innovate to Dominate: The Rise of the Chinese Techno-Security State (Cornell University Press, 2022). He was based Hong Kong, China, and Japan from the mid-1980s to 2002 covering political, economic, and strategic developments in Greater China and East Asia. Dr. Cheung has a PhD in War Studies from King's College, London.

Dr. Sunami Atsushi is the President of Sasakawa Peace Foundation (SPF), Executive Advisor to the President and Visiting Professor, National Graduate Institute for Policy Studies (GRIPS); Special Fellow, Asia Pacific Foundation of Canada; and Visiting Professor, Research Organization for Nano & Life Innovation, Waseda University. He conducts research in maritime policy as well as science, technology, and innovation policy. He has served as Co-Chair of the Japanese National Commission for UNESCO, Ministry of Education, Culture, Sports, Science and Technology; Member of the Advisory Panel on Economic Security Legislation, Cabinet Secretariat; and Member of the Basic Policy Subcommittee, Committee on the National Space Policy, Cabinet Office. He graduated with a PhD in Political Science and a Master of International Affairs (MIA) from Columbia University, and with a B.S. in Foreign Service (BSFS) from Georgetown University. His recent publications and articles include "China as a Hegemonic Power over Advanced Technology," *International Affairs* (February 2022); "Key to the Sustainable Development of the Indo-Pacific," *International Development*

Journal (June 2021); and *Research on Ocean Issues in East Asia : Towards a New Era in Coordination between Japan and China* (April 2020).

Dr. Malcolm Davis joined ASPI as a Senior Analyst in Defence Strategy and Capability in January 2016. Prior to this he was a Post-Doctoral Research Fellow in China-Western Relations with the Faculty of Society and Design at Bond University from March 2012 to January 2016. He has worked with the Department of Defence, both in Navy Headquarters in the Strategy and Force Structure area, and with Strategic Policy Division in the Strategic Policy Guidance from November 2007 to March 2012. Prior to this appointment he was a Lecturer in Defence Studies with Kings College London at the Joint Services Command and Staff College, in Shrivenham, UK, from June 2000 to October 2007. He holds a PhD in Strategic Studies from the University of Hull as well as two Masters degrees in Strategic Studies, including from the Australian National University's Strategic and Defence Studies Centre. His main research focus is on defence strategy and capability development, space policy, military technology, and the future of warfare.

Dr. Michael Raska is an Assistant Professor and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University in Singapore. His research interests focus on defence and military innovation, emerging technologies and strategic competition, and cyber warfare in East Asia. He is the author of *Military Innovation and Small States: Creating Reverse Asymmetry* (Routledge, 2016) and co-editor of *Defence Innovation and the 4th Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications* (Routledge, 2022), and *Security, Strategy, and Military Change in the 21st Century: Cross-regional Perspectives* (Routledge, 2015). His academic publications include articles in journals such as the *Journal of Strategic Studies, Strategic Studies Quarterly, PRISM - Journal of Complex Operations, Journal of Indo–Pacific Affairs, and Sirius - Journal of Strategic Analysis*. He has contributed chapters in edited volumes in collaboration with the Norwegian Institute for Defence Studies (IFS), International Institute for Strategic Studies (IISS), European Union Institute for Security Studies (EUISS), Center for New American Security (CNAS), University of California Institute on Global Conflict and Cooperation (IGCC), and Swedish Defence University (SEDU). He holds a PhD (2012) from the Lee Kuan Yew School of Public Policy, National University of Singapore, where he was a recipient of the NUS President's Graduate Fellowship.

Dr. Ivan V. Danilin is the Head of Science and Innovation Department at Primakov National Research Institute of World Economy and International Relations (IMEMO). He is also the Associate Professor at MGIMO University and the lecturer at several other prominent Russian research universities. In 2010-2015 Dr. Danilin served as a part-timer at innovation departments of biggest Russian power sector companies – ROSATOM and ROSSETI. Since 2010s he took part in the discussions and development of all major Russian innovation policy measures and documents, including the Russian National Technology Initiative, Strategy for Science and Technological Development of the Russian Federation, Concept for the International Science and Technology Cooperation of the Russian Federation. Dr. Danilin serves on board of several federal and corporate expert bodies, including that of the Russian Ministry of Science and Higher Education and State Duma (lower chamber of Russian Parliament). His current research focuses on economic aspects of the digital transformation and associate governance issues and the U.S.-China global technology conflict (including implications for the international high-tech markets and IR). He is author of more than 100 academic publications and more than 20 analytic reports.

NIDS International Symposium on Security Affairs

Technological Innovation and Security: The Impact on the Strategic Environment in East Asia

Wednesday, December 8, 2021 Online

9:00-11:00 **Session 1: Perspectives of the U.S., Japan, and China**

Chair: **Mr. Hyodo Shinji** (Director, Policy Studies Department, NIDS)

Moderator: **Col. Imafuku Hirofumi** (Head, Military Strategy Division, NIDS)

Speakers:

Mr. Bryan Clark (Senior Fellow & Director, Center for Defense Concepts and Technology, Hudson Institute)

Dr. Fujita Motonobu (Policy Coordinator, Technology Policy Office, Technology Strategy Division, Department of Technology Strategy, Acquisition, Technology and Logistics Agency [ATLA]; Visiting Fellow, RAND Center for Asia Pacific Policy [CAPP])

Dr. Tai Ming Cheung (Director, Institute on Global Conflict and Cooperation [IGCC], University of California)

Discussant: **Mr. Iida Masafumi** (Head, America, Europe, and Russia Division, NIDS)

11:10-12:00 **Keynote Speech**

Dr. Sunami Atsushi (President, Sasakawa Peace Foundation [SPF]; Executive Advisor to the President & Director, Science for RE-designing Science, Technology and Innovation Policy [SciREX] Center, National Graduate Institute for Policy Studies [GRIPS])

14:00-16:00 **Session 2: Perspectives of Australia, Singapore, and Russia**

Chair: **Mr. Hyodo Shinji** (Director, Policy Studies Department, NIDS)

Moderator: **Col. Shimazu Takaharu** (Senior Fellow, Military Strategy Division, NIDS)

Speakers:

Dr. Malcolm Davis (Senior Analyst, Australian Strategic Policy Institute [ASPI])

Dr. Michael Raska (Assistant Professor, S. Rajaratnam School of International Studies [RSIS], Nanyang Technological University)

Dr. Ivan V. Danilin (Head, Department of Science and Innovation, Institute of World Economy and International Relations [IMEMO], Russian Academy of Sciences)

Discussant: **Mr. Akimoto Shigeki** (Senior Fellow, Policy Simulation Division, NIDS)

ISBN: 978-4-86482-111-7

The National Institute for Defense Studies
Ministry of Defence