July 2021

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

JEFFREY W. HORNUNG, SCOTT SAVITZ, JONATHAN BALK, SAMANTHA MCBIRNEY, LIAM MCLANE, VICTORIA M. SMITH

Preparing Japan’s Multi-Domain Defense Force for the Future Battlespace Using Emerging Technologies

Numerous rapidly advancing and emerging technology areas—including artificial intelligence (AI), unmanned systems, and directed-energy weapons—will likely affect how defense operations are conducted in the future. A critical challenge for any nation’s defense forces is how to allocate investments across diverse technologies in the decades ahead to be prepared for various types of future operations, including both gray zone situations and contingencies.[1] In this Perspective, we discuss considerations for the Japanese Ministry of Defense (MOD) as it considers possible investments in rapidly advancing and emerging technology areas to help the Self-Defense Forces (SDF) address future challenges.

RAND CORPORATION

Rapidly Advancing and Emerging Technology Areas

Many rapidly advancing and emerging technology areas can potentially shape future warfare. There is always room to dispute which areas should be included in such a list or where the boundaries are between different areas. For our purposes here, we focus on a broad spectrum of technology areas under two headings: information technology and physical systems. We enumerate and briefly define these areas in the table on the next page.

Advances in These Technology Areas in Other Countries

The fact that there are numerous rapidly advancing and emerging technology areas matters for Japan because other nations are simultaneously adapting these technology areas with specific military applications in mind.

In recent decades, European countries have been increasing research and development efforts in several of these technology domains—specifically, additive manufacturing (Johnston, Smith, and Irwin, 2018), autonomy (Kott et al., 2018), big data (Kim, Trimi, and Chung, 2014), biotechnology (Mikulic, 2021; Organisation for Economic Co-operation and Development, 2009), nanotechnology (Dong et al., 2016), and the three quantum technology areas (Srivastava, 2019). As a result, Europe has become known as a prominent global leader in each space. Various countries in Europe are focused on increasing government spending on both foundational research and development (Parkinson, 2018), in addition to advancing technology-specific initiatives that foster collaboration between various sectors. For example, there are initiatives in Europe directed at building satellite constellations for secure government and military communications, as well as several efforts focused on quantum technologies (Fouquet and Drozdiak, 2020; Srivastava, 2019). And although counting the total number of publications, patents, and related citations over a given period is merely one of many ways to gauge impact, the number continues to rise in these technology areas in Europe as well (Dong et al., 2016).

Russia is also investing in these domains. For example, Russia is pursuing the development of hypersonic weapons, partly as a response to U.S. missile defense deployments, both domestically and closer to Russia. Several recent and successful tests have reflected Russia's commitment to further development of these weapon systems and their underlying technologies (Sayler, 2021). Simultaneously, Russia has focused on modernizing enhanced electronic warfare capabilities to enable complex jamming and anti-access/area denial operations. Enhanced electronic warfare can provide Russia with asymmetric capabilities and force enablers or multipliers to engage with the North Atlantic Treaty Organization's eastern flank (McDermott, 2017).

Abbreviations

AI	artificial intelligence
DoD	U.S. Department of Defense
EW	electronic warfare
ISR	intelligence, surveillance, and reconnaissance
MOD	Ministry of Defense
PLA	People's Liberation Army
SDF	Self-Defense Forces

Technology Areas

Technology Area	Definition
Information technology	
Advanced telecommunication networks	Wireless telecommunications with improved hardware, expanded architecture, and new operating procedures to increase capacity and capabilities; often characterized as 5th-, 6th-, and 7th-generation hardware
Artificial intelligence (AI)	Computer systems capable of human-level cognition, including machine learning
Autonomy	The ability of systems to operate with limited or no human supervision
Big data	The ability to handle vast data sets and transform them into useful information
Enhanced cyber warfare	The use of computer code to infiltrate an adversary's information technology networks, enabling surveillance, disruption, and degradation; also includes defenses against such attacks
Enhanced electronic warfare (EW)	The use of the electromagnetic spectrum to disrupt, jam, degrade, or otherwise affect the other side's systems; also includes defenses against such attacks
Quantum communications	The use of the subfield of physics called *quantum mechanics* (involving the probabilistic behaviors of subatomic particles) to make tamper-evident communications
Quantum computing	The use of quantum-mechanical properties to make faster computers
Quantum sensing	The use of quantum-mechanical properties to enhance detection and characterization
Physical systems	
Additive manufacturing	The process of building three-dimensional structures as a series of thin layers; often referred to as *three-dimensional printing*, but it also includes four-dimensional printing, in which a printed structure is designed to change shape when subjected to stimuli
Biotechnology	The production and use of advanced materials derived from living things; military applications include improved medical treatment of injuries; biologically based sensors; and enhanced warfighter cognition, alertness, and strength
Directed-energy weapons	Systems that use intense electromagnetic radiation, such as lasers or microwave-energy bursts, to target adversary systems or personnel
Emerging space	The increasing ability to deploy numerous, multi-mission, compact, low-cost satellites into low Earth orbit
Hypersonic glide vehicles	Vehicles that glide along the edge of the atmosphere at speeds exceeding Mach 5 (6,200 km per hour) and then descend to strike a target; they are particularly useful against fleeting targets or to overcome missile defenses
Microelectronics	The increasingly advanced capabilities of small integrated circuits, which rapidly increases computing power per unit area
Nanotechnology	The manipulation and use of materials with structures in the size range of 1-billionth to 100-billionths of a meter; these materials can evince unusual strength, durability, density, reactivity, and sensitivity
Unmanned vehicles	Vehicles that do not contain humans controlling them and instead may be remotely controlled or have varying degrees of autonomy

Despite its advances across some of these emerging technologies of interest, Russia has not risen to prominence in all 17 areas. For instance, when it comes to AI and big data, Russia has lagged behind both the United States and China, producing fewer academic papers and innovative applications (Polyakova, 2018). More broadly, the United States and China have surpassed Russia as hubs of technological development (Dobbins, Shatz, and Wyne, 2019).

Although both Europe and Russia are making significant strides in several of these emerging technology areas, there are multiple reasons why Japan should not be overly preoccupied with either Europe or Russia. Most notably, European nations are U.S. allies, so there is little to no concern over the chance that Europe will utilize its technological advances against Japan militarily. And although Russia is ramping up efforts in hypersonic weapons and cyber and electronic warfare, there is still a rather significant differential in technological capabilities between Russia and the United States when considering the 17 technology areas collectively. This means that the United States—and, by extension, Japan—has probable cause to be less concerned about developments in Russia.

The same cannot be said about China. China is increasingly viewed as a near-peer adversary to the United States because of the magnitude of China's technology investments, the breadth of technology investments across all 17 areas, and the propensity to utilize technologies against the United States and U.S. interests. Multiple countries all over the world are investing in these technologies and making significant advances, but China is the one country that not only is most likely to succeed at becoming globally dominant but also has the greatest potential to use said technologies against the United States and its interests. Thus, understanding that the Japanese government does not recognize China as an adversary, the RAND Corporation researchers responsible for this Perspective decided that China is an appropriate baseline against which to consider technological advancements.

For the past three decades, China has made impressive progress in a comprehensive military modernization effort. This effort has been driven by evolving military strategy and operational concepts designed to make the People's Liberation Army (PLA) more technologically advanced and better suited to fight wars. Since its founding, the PLA's underlying military strategy has been that of active defense (Fravel, 2019). The PLA's strategy has focused on China's traditional core mission of maintaining sovereignty, security, and territorial integrity. Although the focus of the strategy has not changed, the military strategic guidelines and operational approaches to the strategy have evolved. In 2015, the guidelines began to focus on winning "informatized local wars," recognizing the centrality of information both as a domain in which war occurs and as the central means to wage conflict when the dominant mode of warfare is confrontation between information-based systems (Burke et al., 2020, p. 5; Engstrom, 2018). Under these strategic guidelines, using networked information systems in all domains becomes a priority, and taking away information superiority from an adversary therefore becomes a primary objective in conflict (Burke et al., 2020, p. 7; Pollpeter, Chase, and Heginbotham, 2017).

Against this backdrop, the PLA has pursued several modernization efforts. As a 2020 U.S. Department of Defense (DoD) report to Congress details, the PLA has been actively modernizing with new technologies and improving its proficiencies across all domains so that it can conduct a variety of air, ground, maritime, space, counterspace, electronic warfare (EW), and cyber operations as a joint force (DoD, 2020, pp. 38–91). Creating a modern joint force necessitates the deployment of increasingly capable equipment, including

- more-modern and more-mobile ground forces with upgraded combat systems
- modern multi-role naval platforms fielding advanced anti-ship, anti-air, and anti-submarine weapons and sensors
- a growing arsenal of unmanned aerial vehicles and more-advanced EW; fighter; airborne early warning and control; and intelligence, surveillance, and reconnaissance (ISR) aircraft
- longer-range and more-accurate conventional cruise and ballistic missiles, including anti-ship ballistic missiles designed to target U.S. aircraft carriers (DoD, 2020, pp. 40–60).

More recently, China has been making strides in advancing its space, cyber, and EW capabilities.

Alongside modernization, the PLA has also undertaken significant organizational changes meant to shift the previously ground force–centric structure in favor of naval, air, and missile forces while concurrently positioning itself to be a more efficient and integrated force for operating in multiple domains. The move that was most important for addressing the primary command and control obstacle to improved jointness was the restructuring of the PLA. In 2016, China established five theater commands with joint operation commands to replace seven PLA Army regions.[2] The change was meant to improve the PLA's ability to conduct long-term planning and preparation for joint military operations. Other significant changes include the creation of the PLA Rocket Force as a full-status service equal to the PLA Army, PLA Navy, and PLA Air Force and the creation of the PLA Strategic Support Force.[3]

Both PLA modernization and organizational changes contribute to the PLA's interest in leveraging technology to fight and win informatized wars. Thus, China has invested heavily and consistently in science and technology, and it is expected to continue to do so in the decades ahead. Although investing in science and technology for military purposes is not new, China's President Xi Jinping has heightened the priority placed on defense technology (Cheung and Mahnken, 2018). China does not simply seek to master and apply new technologies; it seeks to become a leader in key technologies that have military potential, such as AI, autonomous systems, advanced computing, quantum information sciences, biotechnology, and advanced materials and manufacturing (DoD, 2020, pp. 144–148; Fox, 2020; Kania and Costello, 2018).

> China does not simply seek to master and apply new technologies; it seeks to become a leader in key technologies that have military potential.

With the informatization of warfare at the core of everything the PLA wants to accomplish, Japan and other states have to take notice. China is very much focused on harnessing technology for military purposes. Its 13th Five-Year Plan (2016–2020), for example, lists several reforms that China is undertaking to increase its competitiveness in key defense industries, including

- quantum communications and computing
- innovative electronics and software
- automation and robotics
- special materials and applications
- nanotechnology
- neuroscience, neural research, and AI (DoD, 2020, p. 141).

Other areas of advanced military capabilities with disruptive potential that China is pursuing include hypersonic weapons, electromagnetic railguns, directed-energy weapons, and counterspace capabilities (DoD, 2020, p. 147). Its efforts today will have profound implications for the types of capabilities the PLA could field in the coming decades. Many of China's short-term goals—such as acquiring larger quantities of conventional land-attack and anti-ship ballistic missiles (with increasingly long ranges); longer-range land-attack and anti-ship cruise missiles; and a host of long-range radar, jamming, anti-satellite, and cyber capabilities—are likely attainable, but goals further into the future are a bit more ambitious (Scobell et al., 2020, p. 88). By 2030, for example, the PLA wants to complete the world's first quantum communications capability, which would include dozens of satellites and ground-based quantum communication networks, and develop a quantum radar capable of receiving critical information about a target, including its shape, location, speed, temperature, and even the chemical composition of its paint (Scobell et al., 2020, pp. 95–96).

The goals that China has set out for itself for the next 30 years may seem ambitious, but China has proven itself capable of marshalling the requisite resources and technologies to make changes that it deems necessary. Although it is possible that economic slowdowns, social instability, large-scale domestic unrest, a North Korean collapse, or other such events could divert China from attaining its goals, planning for possible PLA success prepares Japan for a worst-case future (for several other scenarios, see Chase et al., 2015, pp. 21–24).

How Japan's Self-Defense Forces Can Use Emerging Technology Areas

Although Japan does not base its defense spending on that of any specific country, given its limited defense budget, Japan needs to make well-informed choices among technology investments in order to ensure that the investments it makes will have the most collective impact. Systems that require limited numbers of personnel are advantageous, given Japan's shrinking population (particularly among young people). Japan can help deter and counter potential aggression from other countries by being more effective in using emerging technology areas. In this section, we describe several key areas in which Japan could focus its efforts.

As Japan anticipates potential threats, a critical challenge will be how to allocate MOD investments across diverse technology areas to be prepared for various types of future operations. We identify the following important takeaways that can help inform investments in building the SDF into a Multi-Domain Defense Force over the next two decades.

First, **developments in some technology areas will enable potential aggressors to have plausible (or implausible) deniability**. The use of cyberattacks, EW, and microwave-burst directed-energy weapons may allow adversaries to take actions without clear evidence of involvement. Some attacks may not even be recognized as having been such. Even if Japanese officials are certain of a specific nation's responsibility for a particular attack, it may be difficult to prove culpability.

Second, **the pace of warfare is dramatically increasing, requiring that systems have even more autonomy**. Such technology areas as autonomy, AI, big data, advanced telecommunications, and quantum computing will push decisionmaking and coordinated action to faster speeds than human beings can manage. The result is that Japan, like other nations, will need to not only employ systems that can decide and act without human intervention but also have the confidence to allow the systems to do so. For example, autonomous systems will be needed to parry many cyber and EW attacks, but by the time a human being is able to grasp the situation, the other side would have an immense advantage. The fact that cyber, EW, and directed-energy weapons can all strike at the speed of light also keeps the pace of conflict at a speed faster than what humans can manage. A further advantage of more-autonomous systems is that they can reduce personnel requirements and associated costs. Employing numerous autonomous systems would be an opportunity for Japan to strengthen its capabilities despite its shrinking population and limited defense budget.

> The fact that cyber, EW, and directed-energy weapons can all strike at the speed of light keeps the pace of conflict at a speed faster than what humans can manage.

Third, **unmanned vehicles will likely play a central role in future warfare**. These vehicles can take on greater risks, and greater payloads, in the absence of personnel. To the degree that they are autonomous (as opposed to being remotely controlled), they can also reduce personnel requirements. Large numbers of unmanned vehicles, each costing a fraction of the cost of a manned platform, can distribute themselves throughout the environment to collect ISR and to counter adversary threats with EW or kinetic strikes. Given how many there are, losing some of these vehicles to enemy attack will be entirely acceptable, still leaving their collective capabilities intact. Such vehicles will operate across multiple domains: air, sea surface, undersea, ground, and space (including dense constellations of compact, relatively inexpensive satellites). They can coordinate with one another across those domains, as well as with manned platforms and fixed installations, as part of an overarching network that enables domain awareness and precise targeting.

Fourth, **long-range, accurate targeting is becoming more available**. Given ubiquitous sensors on unmanned vehicles in multiple domains (including space) and the ability of weapons to rapidly interpret data for terminal guidance onto their targets, it is increasingly possible for long-range attacks to hit their targets very precisely, achieving specific effects without wasting weapons and while minimizing the risk of collateral damage.

Fifth, **network security and disruption of the other side's networks will be increasingly central to conflict**. As each side increasingly uses networks of unmanned and manned systems for C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) and targeting, it is critical to protect those networks through EW and cyber defenses. Although networks can survive the loss of individual nodes, damage to network functioning and connectivity can degrade overall capabilities. For Japan, strengthening cyber and EW defenses is also important for ensuring interoperability with U.S. forces; the United States will be able to integrate its networks with Japan's only if it has confidence that doing so would not lead to backdoor infiltration of its own networks. Effective cyber and EW attacks can fragment adversary networks into disparate pieces that are incapable of coordinated action.

In addition to planning for the traditional air, ground, and maritime domains of conflict, there is a need to treat the electromagnetic, space, and cyberspace domains as central to success.

Sixth, **the domains of conflict are expanding**. In addition to planning for the traditional air, ground, and maritime domains of conflict, there is a need to treat the electromagnetic, space, and cyberspace domains as central to success. These domains have existed for decades or longer, but they are becoming more important and pervasive; success in the traditional domains depends on success in the newer ones. Moreover, although conflict has always had a strong cognitive component, the advent of new technologies enables each side to influence the other's perceptions more effectively than before, elevating cognitive considerations.

Seventh, building on the previous point, **technology areas relevant to the information domain are increasingly important**. Although precise advances are difficult to predict, Japan can expect potential adversaries to continue focusing significant efforts on controlling the information environment and associated technology domains. Other nations may seek to use various technology areas in all phases of conflict to adversely influence Japanese cognitive functions and shape international public opinion. Japan should be prepared to deal with massive misinformation campaigns by being able to quickly identify misinformation—ideally, before broad dissemination—and by educating the public about how to properly identify misinformation and source accurate information on an individual level. Japan has the advantage of being able to partner with the United States and other democratic nations to understand the dynamics of information flow and how to influence it.

Eighth, **deception can play a central role in the SDF's future success**. Naturally, deception has been ubiquitous in warfare for thousands of years. However, emerging technology areas enable more-capable deception at the same time that knowledge of the battlespace becomes more critical to effective targeting. The emergence of unmanned vehicles that can serve as decoys, together with the growing capabilities of cyber, EW, and AI technologies to manipulate perceptions, can greatly increase the ability of either side to deceive the other. When a country can couple high-signature physical decoys with autonomous cyber, EW, and AI systems to inject false information streams into adversary networks, that adversary experiences confusion that leads to worse decisionmaking and critical delays. There are also opportunities to be exploited from the fact that AI can make mistakes that a human never would—for example, misidentifying a photo of a panda as being a gibbon (Goodfellow et al., 2017). Moreover, once an adversary suspects that it is being deceived, even accurate information may be ignored, or acted on only after a delay that allows it to be corroborated. When an adversary organization's commands, personnel, and information technology systems are receiving conflicting information, or perceiving it differently, the resulting tensions can degrade military performance and coordination. In a battlespace in which real-time, accurate knowledge is central to effective targeting, deception can make an immense difference in reducing an adversary's overall capabilities.

Finally, **additive manufacturing, nanotechnology, microelectronics, advanced telecommunication networks, directed-energy weapons, and biotechnology can play valuable supporting roles**. Although other technology areas (cyber, EW, big data, autonomy, unmanned systems, emerging space, and AI) are likely to play primary roles in future warfare, others can be expected to play valuable supporting roles. For example, additive manufacturing can enable on-demand printing of parts and unmanned vehicles from bulk materials, which can reduce logistical requirements on ships or at remote locations. Advances in microelectronics and telecommunications can serve as the hardware backbone on which complex networks employing AI, big data, and autonomous systems rely. Directed-energy weapons can be used to dazzle or disable key sensors and other electronics. Biotechnology can aid in medical treatment and enhance individuals' physical or cognitive capabilities.

Considerations in Shaping Technology Investment Portfolios

Many of the types of technology areas that Japan's MOD could benefit from do not require especially costly investments, compared with the costs of building, maintaining, and operating large manned platforms. Some of these technology areas primarily require investments in personnel who can design and oversee development of AI, big-data, The commercial sector is becoming more interested in defensive cyber capabilities as the threat of cyberattacks, including ransomware, increases from both state and non-state actors.

autonomous, cyber, and EW systems. Although these also require some software and hardware purchases, the overall cost is likely to be lower than that of acquiring, operating, maintaining, and providing personnel for a squadron of aircraft or a fleet of ships.

In addition, Japan can leverage commercial interest and investments in key technology areas to aid in their development and operationalization. Emerging space constellations provide valuable services for the commercial market in remote sensing, broadband communications, and environmental monitoring. Likewise, unmanned systems satisfy many commercial needs, such as monitoring undersea infrastructure, reducing personnel requirements for many tasks, and providing services for an aging population. Nanotechnology can be used to contribute to such fields as medicine and construction, advanced telecommunications can improve the speed and reliability of civilian networks, and additive manufacturing is already being used by manufacturers to streamline production. In the information technology domain, AI, big data, and autonomy can help businesses increase their efficiency, capabilities, and profits. The commercial sector is also becoming more interested in defensive cyber capabilities as the threat of cyberattacks, including ransomware, increases from both state and non-state actors. Additionally, as a result of trends in miniaturization, increased processing speed with lower power requirements, and software-defined circuitry, microelectronics anchor many of the technology areas mentioned in this paper. In all these cases, technology areas that are the focus of considerable private-sector investment can be harnessed by the MOD. Rather than investing in developing the underlying technology areas, what the MOD needs to do is tailor these technologies to particular uses; recruit, hire, retain, and train individuals with the requisite skill sets; and incorporate these technology areas into policy, doctrine, training, and exercises.

Similarly, Japan may benefit from the potential to exploit other nations' organizational weaknesses. In the future, adversaries will likely emphasize using the full battlespace, conducting operations, and striving for effects across domains. Doing so will require these nations to integrate information and capabilities across the physical and informational domains while synchronizing with other lines of effort in a conflict. This will be an enormous undertaking that makes such nations vulnerable to potentially multiple points of failure. Concerted cyber and EW attacks that degrade the ability of adversary systems, people, and services to coordinate could help shatter the other side's overall capabilities. The pervasive use of deception—using coordinated cyber and EW attacks, laser attacks on sensors, kinetic attacks against ISR nodes, and unmanned decoys with accentuated signatures—can have particularly deleterious effects on a highly integrated network that is meant to provide shared situational awareness. Injecting false information into some parts of the network can lead to confusion and inter-service friction as different services disagree about what is happening, contributing to conflict and mutual mistrust. As people and organizations begin to question the veracity of information from particular systems—blaming sensors, big-data analytics, AI systems, individual human operators, or commanders in other services—they will also be more inclined to dismiss accurate information and to selectively act on information that reinforces their existing biases. Moreover, these people and organizations may delay particular actions until their preferred sources of information provide confirmation, impeding their ability to keep up with the pace of the conflict. Such delays can be exacerbated by introducing cyber and EW weapons that simply slow down information technology; the effects might be so hard to distinguish from normal system issues that the attacks would go unnoticed.

Other technology areas may be lesser priorities for MOD investments. For example, quantum computing, sensing, and communications all hold promise in contributing to future defense operations. However, these technology areas are expensive, and they may take decades to mature to the point that they are viable for widespread use in battlefield operations.

Closing Remarks

Given the number and diversity of technology areas with the potential to have a large impact on future warfare, Japan faces challenges in determining how best to invest its resources in technology development to make the future SDF more effective. The analysis in this paper can inform those choices, enabling Japan to more capably deter and counter possible aggression from a future adversary that can employ diverse technology areas.

Notes

[1] A 2019 RAND Corporation report defines the *gray zone* as "an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events" (Morris et al., 2019, p. 8).

[2] The new commands are the Eastern, Southern, Western, Northern, and Central theater commands.

[3] Together, these changes demonstrate the PLA's focus on missiles and on space, cyber, electronic, and psychological warfare missions and capabilities.

References

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts*, Santa Monica, Calif.: RAND Corporation, RR-A394-1, 2020. As of November 30, 2020: https://www.rand.org/pubs/research_reports/RRA394-1.html

Chase, Michael S., Jeffrey Engstrom, Tai Ming Cheung, Kristen A. Gunness, Scott Warren Harold, Susan Puska, and Samuel K. Berkowitz, *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (PLA)*, Santa Monica, Calif.: RAND Corporation, RR-893-USCC, 2015. As of December 3, 2020: https://www.rand.org/pubs/research_reports/RR893.html

Cheung, Tai Ming, and Thomas G. Mahnken, eds., *The Gathering Pacific Storm: Emerging U.S.-China Strategic Competition in Defense Technological and Industrial Development*, Amherst, N.Y.: Cambria Press, 2018.

Dobbins, James, Howard J. Shatz, and Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses*, Santa Monica, Calif.: RAND Corporation, PE-310-A, 2019. As of May 12, 2021: https://www.rand.org/pubs/perspectives/PE310.html

DoD—*See* U.S. Department of Defense.

Dong, Haiyan, Yu Gao, Patrick J. Sinko, Zaisheng Wu, Jianguo Xu, and Lee Jia, "The Nanotechnology Race Between China and USA," *Materials Today*, April 12, 2016.

Engstrom, Jeffrey, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, Santa Monica, Calif.: RAND Corporation, RR-1708-OSD, 2018. As of November 30, 2020: https://www.rand.org/pubs/research_reports/RR1708.html

Fouquet, Helene, and Natalia Drozdiak, "Europe Wants Its Own Alternative to Musk's Starlink Network," *Bloomberg*, December 16, 2020.

Fox, Christine, *An Entwined AI Future: Resistance Is Futile*, Laurel, Md.: Johns Hopkins Applied Physics Laboratory, 2020.

Fravel, M. Taylor, *Active Defense: China's Military Strategy Since 1949*, Princeton, N.J.: Princeton University Press, 2019.

Goodfellow, Ian, Nicolas Papernot, Sandy Huang, Rocky Duan, Pieter Abbeel, and Jack Clark, "Attacking Machine Learning with Adversarial Examples," *Open AI* blog, February 24, 2017.

Johnston, Trevor, Troy D. Smith, and J. Luke Irwin, *Additive Manufacturing in 2040: Powerful Enabler, Disruptive Threat*, Santa Monica, Calif.: RAND Corporation, PE-283-RC, 2018. As of May 12, 2021: https://www.rand.org/pubs/perspectives/PE283.html

Kania, Elsa B., and John K. Costello, *Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership*, Washington, D.C.: Center for a New American Security, September 12, 2018.

Kim, Gang-hoon, Silvana Trimi, and Ji-hyong Chung, "Big Data Applications in the Government Sector: A Comparative Analysis Among Leading Countries," *Communications of the ACM*, Vol. 57, No. 3, 2014, pp. 78–85.

Kott, Alexander, Ryan Thomas, Martin Drašar, Markus Kont, Alex Poylisher, Benjamin Blakely, Paul Theron, Nathaniel Evans, Nandi Leslie, Rajdeep Singh, Maria Rigaki, S. Jay Yang, Benoit LeBlanc, Paul Losiewicz, Sylvain Hourlier, Misty Blowers, Hugh Harney, Gregory Wehner, Alessandro Guarino, Jana Komárková, and James Rowell, *Toward Intelligent Autonomous Agents for Cyber Defense: Report of the 2017 Workshop by the North Atlantic Treaty Organization (NATO) Research Group IST-152-RTG*, Prague: U.S. Army Research Laboratory, ARL-SR-0395, April 2018.

McDermott, Roger N., *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, Tallinn: Estonian Ministry of Defence, International Centre for Defence and Security, September 2017.

Mikulic, Matej, "Biotech Research and Development Expenditure in Selected Countries in 2018," webpage, Statista, January 8, 2021. As of May 12, 2021:
https://www.statista.com/statistics/379945/country-biotechnology-company-rd-spending

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica, Calif.: RAND Corporation, RR-2942-OSD, 2019. As of April 30, 2021:
https://www.rand.org/pubs/research_reports/RR2942.html

Organisation for Economic Co-operation and Development, *OECD Science, Technology and Industry Scoreboard 2009*, Paris, 2009.

Parkinson, Stuart, "EU Moves into Military Science and Technology," *SGR Newsletter*, No. 46, Winter 2018, pp. 7–9.

Pollpeter, Kevin L., Michael S. Chase, and Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, Santa Monica, Calif.: RAND Corporation, RR-2058-AF, 2017. As of November 30, 2020:
https://www.rand.org/pubs/research_reports/RR2058.html

Polyakova, Alina, *Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare*, Brookings Institution, November 15, 2018.

Sayler, Kelley M., *Hypersonic Weapons: Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, R45811, April 26, 2021.

Scobell, Andrew, Edmund J. Burke, Cortez A. Cooper III, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J. D. Williams, *China's Grand Strategy: Trends, Trajectories, and Long-Term Competition*, Santa Monica, Calif.: RAND Corporation, RR-2798-A, 2020. As of November 30, 2020:
https://www.rand.org/pubs/research_reports/RR2798.html

Srivastava, Smriti, "Top 10 Countries Leading in Quantum Computing Technology," *Analytics Insight*, December 14, 2019.

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress*, Washington, D.C.: Office of the Secretary of Defense, September 2020.

About the Authors

Jeffrey W. Hornung is a political scientist at the RAND Corporation. He specializes in Japanese security and foreign policies, East Asian security issues, and U.S. foreign and defense policies in the Indo-Pacific region. Hornung holds a Ph.D. in political science.

Scott Savitz is a senior engineer at the RAND Corporation. Much of his research focuses on how to improve the effectiveness and resilience of operational forces, as well as the impact of reallocating resources among those forces. Savitz holds a Ph.D. in chemical engineering.

Jonathan Balk is a research assistant at the RAND Corporation with interests in emerging technologies, space systems, and policy analysis. He holds a bachelor's degree in aerospace engineering.

Samantha McBirney is an associate engineer at the RAND Corporation. Her primary research interests are in medical readiness, medical logistics, emerging technologies (and how they are used by near-peer adversaries), and pharmaceutical supply chains. She holds a Ph.D. in biomedical engineering.

Liam McLane is a research assistant at the RAND Corporation with interests in cost estimation, analysis of government contracting mechanisms, and data collection and analysis. He holds a bachelor's degree in economics and political science.

Victoria M. Smith is a research assistant at the RAND Corporation with interests in modeling, cost estimation, and emerging technologies. She holds a bachelor's degree in economics and international relations.

Acknowledgments

We would like to thank several people for helping us conduct this research. Agnes Gereben Schaefer and Michelle Platt were our principal contact points for ensuring that we were fulfilling the necessary RAND requirements and keeping the project within budget. Jim Powers, the RAND National Security Research Division quality assurance manager, read the paper and ensured that it met RAND quality assurance standards. Laura Poole, Susan Arick, Natalie Richards, Rosa Maria Torres, and Johanna Whittaker helped make sure our references were in order, and Allison Kerns served as copy editor.

In addition, we benefited from the expert insights provided by numerous RAND colleagues: Nathan Beauchamp-Mustafaga, Steven Berner, Michael Bond, Benjamin Boudreaux, Jennifer Brookes, Kyle Bunch, Cortez Cooper, Jim Dimarogonas, Jeffrey Engstrom, Cristina Garafola, Edward Geist, Daniel Gonzales, Derek Grossman, Gavin Hartnett, Alex Hou, John Luke Irwin, Christian Johnson, Eric Landree, Bradley Martin, Jason Mastbaum, Mace Moesner, Jared Mondschein, Thoa Liz Nguyen, Chad Ohlandt, Edward Parker, James Ryseff, Troy Smith, Eder Sousa, Randall Steeb, Danielle Tarraf, Padmaja Vedula, and Rand Waltzman.

Finally, we would like to thank the officials at the Japanese Ministry of Defense's Strategic Planning Division, which sponsored this Perspective, and at Mitsubishi Research Institute for helping provide critical input during the research process.

About This Perspective

A variety of emerging technology areas will likely affect how defense operations are conducted in the future. Japan's Self-Defense Forces can employ these technology areas to improve effectiveness; the forces also need to be prepared to address threats from other nations that might use the technology areas against Japan. The Strategic Planning Division of the Japanese Ministry of Defense sponsored the RAND Corporation to analyze how emerging technology areas may shape military operations in the future.

RAND National Security Research Division

This research was sponsored by the Strategic Planning Division of Japan's Ministry of Defense and conducted within the International Security and Defense Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

For more information on this publication, visit www.rand.org/t/PEA1157-1.