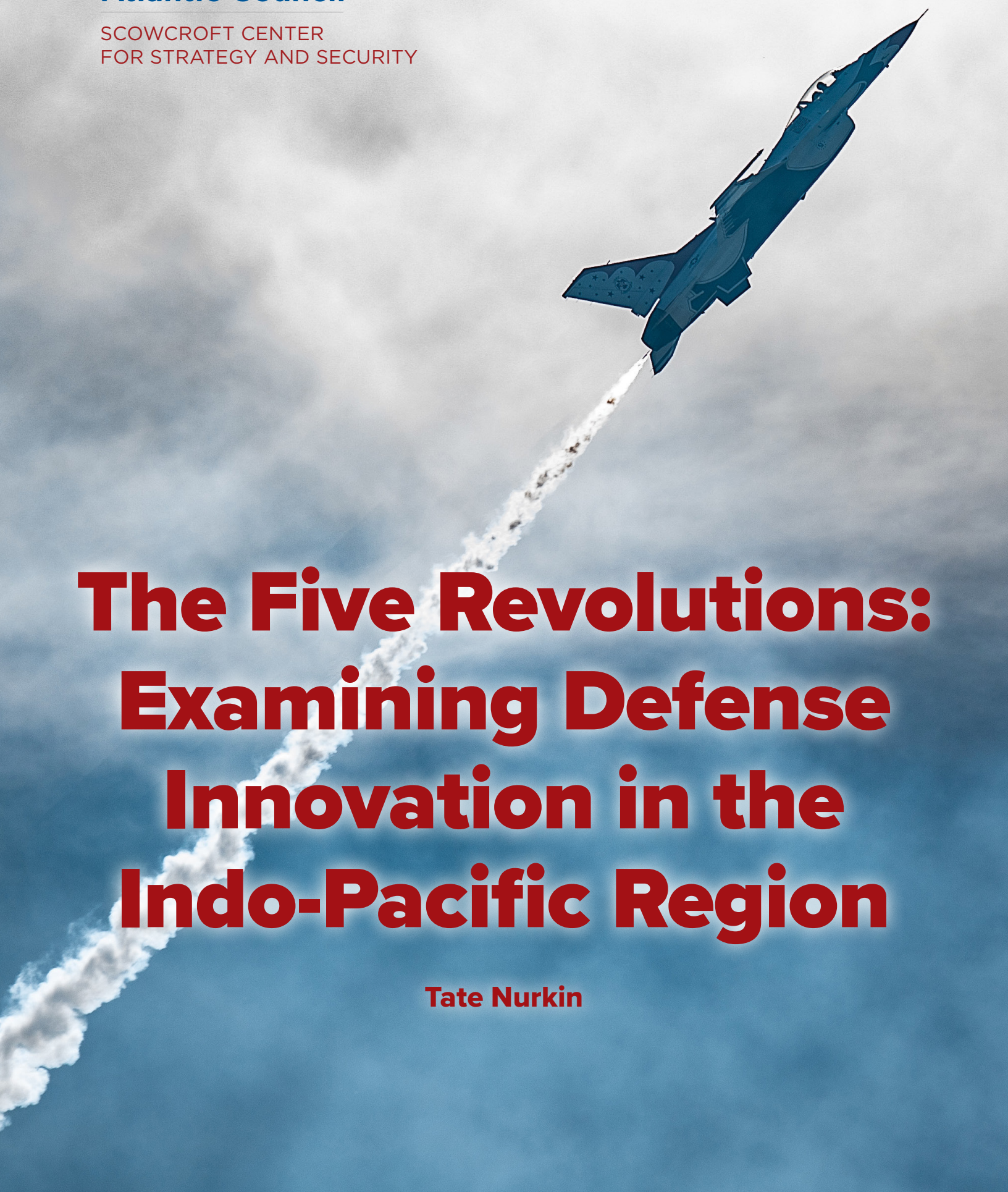
Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY



The Five Revolutions: Examining Defense Innovation in the Indo-Pacific Region

Tate Nurkin

Scowcroft Center for Strategy and Security

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Forward Defense

Forward Defense (*F*D) helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces *Forward*-looking analyses of the trends, technologies, and concepts that will define the future of warfare, and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, *Forward* Defense develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition.

With Thanks To

This project was conducted under the supervision of *F*D Deputy Director Clementine Starling and Assistant Director Christian Trotti, and was enabled by research support from *F*D interns Olivia Popp and Julia Siegel.

The Five Revolutions: Examining Defense Innovation in the Indo-Pacific Region

Tate Nurkin

ISBN-13: 978-1-61977-142-0

Cover: The US Air Force Thunderbirds perform during the Thunder and Lightning Over Arizona at Davis-Monthan Air Force Base, Arizona, March 23, 2019. *Source:* US Air Force photo by Staff Sgt. Jensen Stidham, US Air Force flickr page. https://www.flickr.com/photos/usairforce/47585680981/

November 2020

Table of Contents

Executive Summary

The Indo-Pacific region has become a center of gravity for innovation in defense technologies and emerging military capabilities.

Assessing the dimensions and relevance of technological innovation across the region requires examination not just of the *what* of technology development, but also the *why*—that is, the prioritized effects militaries seek to achieve.

This report seeks to address both the *what* and the *why*, while also offering insight into the *so what* of how technology- and capability-development activities are changing the nature of competition and conflict in the region.

It begins by describing a series of strategic and operational forces and tensions that are shaping innovation priorities in the region, especially for China and the four nations of the reinvigorated Quadrilateral Security Dialogue (or "Quad"): the United States, Australia, Japan, and India.

- **China** is at the center of geopolitical concern and, as a result, of defense modernization and innovation efforts among many states across the region, due to its aggressive behavior and the nature and pace of its military modernization effort.
- The threat environment for most states is expanding to include **a variety of traditional and nontraditional security challenges** including the prevalence of, and continued potential for, gray-zone contingencies. Different states view these challenges with different levels of urgency and intensity, but the view is pervasive that the Indo-Pacific security environment has "deteriorated more rapidly than anticipated" over the last several years.[1]
- Activity in and *across* **three "new" domains of space, cyber, and the electromagnetic spectrum** is a powerful driver not just of military capabilities and military competition, but also of how militaries in the region organize to better operate in a multi-domain environment.

The intersection of these drivers with one another and the rapidly advancing Fourth Industrial Revolution (4IR) has led to a "blurring" of lines between military domains, military and non-military technologies and activities, and states of peace and conflict. This blurring phenomenon is complicating efforts to detect and then shape, deter, and respond to a diversifying set of regional challenges.

To help capture and monitor defense-technology and military-capability development efforts, the report articulates a "Five Revolutions" framework, tasks complicated by the pace, scale, and diversity of innovation efforts related to emerging and 4IR technologies. This framework focuses analysis on the intended *effects* of technology development, rather than on the technologies themselves.

Specifically, the framework tracks efforts to achieve step-changes—or revolutions—in five broad capability areas, including

1. perception, processing, and cognition;
2. human and machine performance;
3. manufacturing, supply chain, and logistics;
4. communications, navigation, targeting, and strike; and
5. cyber and information operations.

The report concludes by summarizing key themes and policy implications of the high-level review of defense-technology development in China, Japan, India, Australia, and across the region. Key takeaways include the following.

- Key technology- and capability-development activities among US allies and Quad partners are focused, first and foremost, on enhancing the ability to detect security threats and challenges that are increasingly difficult to anticipate or recognize.
- Building improved situational awareness and multi-mission capabilities will be a priority as militaries seek to become more agile and better equipped to respond to a diverse set of possible threats and challenges.
- Improving the range of possible responses available to operators and decision-makers—including more non-kinetic capabilities—will offer militaries more options for crafting appropriate responses to traditional and nontraditional contingencies in the region.
- Technology development will also be centered on building more lethal forces, to enhance deterrence and to ensure the capacity to fight in a high-intensity kinetic conflict, even if such a conflict is less likely than other, more subtle, challenges.
- Collaboration between the United States and its allies on defense-technology development—as well as other areas, such as operational concepts, training, technological standards, and ethics and safety of technology use—should be encouraged and expanded in order to ensure a higher degree of interoperability, especially in the new domains of cyber, space, and the electromagnetic (EM) spectrum.

1 "2020 Defence Strategic Update," Australian Department of Defence, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf.

The Five Revolutions: Examining Defense Innovation in the Indo-Pacific Region

I. Introduction and Overview: The Indo-Pacific as Center of Gravity of Defense Innovation

The year 2020 has been difficult. Polities, economies, and societies throughout the world have sought to manage and contain the layered and cascading consequences of the still-mostly uncontained coronavirus pandemic.

However, in the narrow area of military technology, 2020 has been an impressive year filled with breakthroughs in emerging and 4IR technologies, and demonstrations of novel capabilities that are progressing—in some cases unexpectedly quickly—along the pathway from the abstract to the operational.

Consider the US Department of Defense's exceptional month running from mid-August to mid-September.

On August 18, an artificial intelligence (AI) agent developed by Heron Systems defeated a human-operated F-16 in a series of five virtual dogfights as part of the final round of the Defense Advanced Research Projects Agency's (DARPA's) AlphaDogfight challenge. The event was an important step forward for, and validation of, the efficacy of high-end autonomous systems with direct implications for the future of human-machine teaming.[2]

Less than a month later, on September 15, the US Air Force (USAF) made a shock announcement that it secretly designed, built, and test flew a real-world prototype fighter jet within twelve months as part of its Next Generation Air Dominance (NGAD) project. The milestone was reached using digital-twinning design technologies that not only greatly reduce development costs and timelines, but also provide the long-sought-after ability to quickly produce adapted designs that integrate advancements in emerging technologies.[3]

Achievements in defense-technology development have not been limited to the United States. Militaries across the Indo-Pacific region are exhibiting a more robust dedication and capacity to exploit the digital transformation enabled by 4IR technologies, and to build advanced platforms and weapons systems that incorporate new energies, advanced propulsion, and materials science.

Whether it is the reveal in May—and now-impending test flight before the end of the year—of Boeing Australia's loyal wingman Airpower Teaming System (ATS) prototype, or the revelation that China tested a fixed-wing drone swarm system in October, or the various milestones achieved related to hypersonic missiles by China, Russia, India, and Japan over the course of the year (among many other compelling examples), evidence is mounting that the Indo-Pacific has emerged as a center of gravity of global military-technological innovation and competition.[4]

II. Drivers of Defense Technology Priorities in the Indo-Pacific

At the core of defense modernization in the region is the digital transformation enabled by 4IR technologies such as AI, cloud computing, virtual and augmented reality, smart sensors, and many more. The savvy application of these technologies is creating new efficiencies and a range of "new possibles" for Indo-Pacific militaries of all sizes. The Australian Department of Defence's "Defence Science and Technology Strategy 2030" paper highlights several of the areas in which this digital transformation—as well as advancements in other emerging technology areas—is having a pronounced effect:

> "The [Australian Defence Force's] ability to understand the operational environment, maneuver and project force will be transformed through advances in sensing, information fusion, and dissemination, artificial intelligence and human-machine partnership. The way Defence sustains its capabilities will

2 Patrick Tucker, "An AI Just Beat a Human F-16 Pilot in a Dogfight—Again," *Defense One,* 20 August 2020, https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/.

3 Marcus Weisgerber, "Revealed: US Air Force Has Secretly Built and Flown a New Fighter Jet," *Defense One*, September 15, 2020, https://www.defenseone.com/technology/2020/09/usaf-jet/168479/.

4 "Boeing Rolls Out First Loyal Wingman Unmanned Aircraft," Boeing, press release, May 5, 2020, https://boeing.mediaroom.com/2020-05-05-Boeing-rolls-out-first-Loyal-Wingman-unmanned-aircraft; Minnie Chan, "China Tests Swarm of 'Suicide Drones' Launched from a Truck and Helicopters," *South China Morning Post,* October 16, 2020, https://www.scmp.com/news/china/military/article/3105670/china-tests-swarm-suicide-drones-launched-truck-and-helicopters.

> be greatly enhanced, increasing platform availability and reducing costs. Technological change will improve our resilience, support a new level of agility in command and control, and give us new options for effects, whether kinetic or in the information domain."[5]

But, this same technology development is also creating risks and challenges, especially as it intersects fully with new operational realities and a changed and still changing Indo-Pacific strategic environment—one that Australia's "2020 Defence Strategic Update" assessed was in the midst of "the most consequential strategic realignment since World War II."[6]

The result has been a blurring of the lines of demarcation separating military domains, military and nonmilitary activities, and states of peace and conflict, all of which has implications for the future of conflict in the region. The 2017 "Joint Doctrine" of the Indian Armed Forces summed up the impact of technological innovation and the blurring it is producing on military operations, describing the future of conflict as "ambiguous, uncertain, short, swift, lethal, intense, precise, nonlinear, unrestricted, unpredictable, and hybrid."[7]

In this environment, anticipating and assessing the technologies and priorities in demand requires an understanding of at least the following high-level strategic and operational drivers of regional technology development.

China's Rise, Chinese Military Modernization, and US-China Competition

China's assertive behavior and advancing military modernization are the primary strategic concern motivating defense strategy and shaping technology and capability investments for many US allies in the Indo-Pacific, particularly the Quad states of Australia and Japan. Even states that are unwilling to identify China specifically as the main strategic concern stress the escalatory effect that intensifying competition between the United States and China is having on regional geopolitical tensions.

For Quad states, though, China's perceived efforts to aggressively press its territorial claims, challenge the regional status quo, and undermine the rules-based order and freedom of the seas has served as a cohering force at both the bilateral and multilateral levels. Even India, which has long been reluctant to be viewed as joining an "anti-China" alignment and faces several other persistent border and internal security challenges, has deepened its engagement with the Quad in the wake of June border violence with China. Indeed, in November 2020, India hosted an expanded Malabar naval exercise that included traditional participants India, the United States, and Japan, as well as Australia, which was participating for the first time in thirteen years.

This change in perception is not yet fully reflected in the ways that the Indo-Pacific Quad states reference China in official government publications. Even Australia and Japan, states that have been less ambiguous in their perspectives on China over the last year, have been hesitant to directly identify China as an adversary or strategic competitor due to their deep—or, in the case of Australia, currently fraught—economic relationships with Beijing.

Australia's "2020 Defence Strategic Update" only mentions China nine times—most of which are paired with references to the United States and to US-China competition. But, there is no confusion about what animates that document, or even "Defense of Japan 2020." As the Australian Broadcasting Corporation pointed out in its coverage of the release of the updated strategy, generic references to "coercion…targeting Australian interests" are less-than-subtle references to the People's Republic of China (PRC).[8]

So, too, are assertions in the document that "military modernisation in the Indo-Pacific has accelerated faster than envisaged."[9] As Zach Cooper and Charles Edel point out in a recent *Foreign Policy* article entitled, "Australia Is Having a Strategic Revolution, and It's All About China," China is the only state in which "there [has] been a serious increase in overall defense spending" over the last five years.[10]

Growing concern about China's activities in the region has fundamentally altered Australia's defense strategy, which is now focused on Australia's "immediate region," ranging from the Northeastern Indian Ocean through Southeast Asia to the Southwest Pacific, rather than the expeditionary

5 "More, Together: Defence Science and Technology Strategy 2030," Australian Department of Defence, October 2020, https://www.dst.defence.gov.au/strategy.

6 "2020 Defence Strategic Update."

7 "Joint Doctrine: Indian Armed Forces," Headquarters Integrated Defense Staff, Ministry of Defence, April 2017, https://ids.nic.in/IDSAdmin/upload_images/doctrine/JointDoctrineIndianArmedForces2017.pdf.

8 Stephen Dziedzic, "Australia's New Defence Strategy Unveils a Significant Strategic Shift in Foreign Policy to Meet New Threats from China," ABC News, July 1, 2020, https://www.abc.net.au/news/2020-07-02/australias-new-defence-strategy-strategic-shift-foreign-policy/12412650.

9 "2020 Defence Strategic Update."

10 Zach Cooper and Charles Edel, "Australia Is Having A Strategic Revolution, and It's All About China," *Foreign Policy,* July 22, 2020, https://foreignpolicy.com/2020/07/22/australia-military-strategy-regional-policy-china/.

operations in the Middle East that have dominated Australia's defense activities in the twenty-first century.[11]

China's Military Modernization and Regional Responses

The nearly three-decades-old effort to transform the People's Liberation Army (PLA) and create a world-class military by 2049 has made impressive progress over the last decade across most components of military capabilities and technology development.

Development, and now deployment, of impressive anti-access/area denial (A2/AD) capabilities has enabled China's ability to better position itself to fight and win regional wars. The PLA Navy's (PLAN) massive shipbuilding campaign is allowing China—especially in conjunction with white hull vessels in the People's Armed Police Force Coast Guard and commercial vessels in China's Maritime Militia—to create mass, which can help it gain the initiative and potentially control in a range of maritime domain contingencies. China is also developing more robust capabilities to protect its growing global concerns, including two in service aircraft carriers and a new joint logistics-support force to facilitate expeditionary operations.[12]

The list of key PLA modernization developments affecting regional military balances and defense priorities is too extensive to be covered completely here. However, the below capability areas are particularly relevant to this paper's analysis.

- **Information dominance:** The ability to ensure the security of its own command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, while also being able to reliably and sustainably hold at risk adversary C4ISR capabilities, is at the core of China's military-modernization effort and approach to winning regional wars, especially under informatized (or highly networked) conditions. Information dominance places a premium on being able to compete effectively in space, the cyber domain, and the electromagnetic spectrum.

- **Anti-ship and hypersonic missiles:** Much has been written about China's DF-21D and DF-26B anti-ship ballistic missiles (ASBMs). They constitute a viable, but likely still vulnerable, capability to target US and allied and partner surface assets, including US aircraft carriers. The display of the DF/CJ-100 anti-ship, ground-launched, and likely hypersonic cruise missile at the October 1, 2019, military parade commemorating the founding of the People's Republic of China appears to be an additional challenge for regional navies.[13]

  In addition, China's hypersonic-missile development program has developed considerable momentum. The display of the DF-17 hypersonic glide-vehicle system in October 2019 was not necessarily a surprise, but it was still an important milestone. Recent online photos of the massive CH-AS-X-13 air-launched anti-ship (possibly hypersonic) missile further reinforce the perception that China has an advantage in hypersonic-weapons technology.[14] So, too, do the spring 2020 reports of a Chinese Academy of Sciences Institute setting a ground test record of a scramjet engine that lasted six hundred seconds.[15] The US X-51A Waverider set the previous record of a two hundred thirty one second scramjet engine burn in 2013.[16]

  The combination of speed, maneuverability, and different launch vectors of China's advanced anti-ship and hypersonic missiles (land- and air-launched, ballistic and non-ballistic trajectories) all pose enhanced—if not entirely new—challenges for regional missile defenses.

- **Discourse power:** China is also developing its "discourse power," or ability to set agendas and narratives internationally, by "influencing the political order and values both domestically and in foreign countries."[17] A September 2020 Atlantic Council Digital Forensics Lab report describes the intent and methods of China's efforts to expand its "discourse power" by leveraging both Chinese-language and Western social media to support its campaign to rewrite international norms, values, and ethics. The intended outcome of

11 "2020 Defence Strategic Update."

12 Chad Peltier, Tate Nurkin, and Sean O'Connor, "China's Logistics Capabilities for Expeditionary Operations," US-China Economic and Security Review Commission, April 15, 2020, https://www.uscc.gov/research/chinas-logistics-capabilities-expeditionary-operations.

13 Sebastian Roblin, "The DF-100 Is China's Biggest Threat to the U.S. Navy," *National Interest*, April 17, 2020, https://nationalinterest.org/blog/buzz/df-100-chinas-biggest-threat-us-navy-145172.

14 H.I. Sutton, "China's New Aircraft Carrier Killer Is World's Largest Air-Launched Missile," *Naval News*, November 1, 2020, https://www.navalnews.com/naval-news/2020/11/chinas-new-aircraft-carrier-killer-is-worlds-largest-air-launched-missile/.

15 Stephen Chen, "Report of Chinese Scramjet Test a Challenge to Most-Advanced Missile Defence Systems," *South China Morning Post*, May 31, 2020, https://www.scmp.com/news/china/science/article/3086804/report-chinese-scramjet-test-challenge-most-advanced-missile.

16 Ibid.

17 Alicia Fawcett, *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition, Atlantic Council*, October 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/10/Chinese-Discourse-Power.pdf.

An artist's concept drawing for the Defense Advanced Research Projects Agency's (DARPA) Gremlins program, which envisions launching groups of unmanned aerial systems (UASs) from existing aircraft to serve ISR and other missions. China is also interested in the military applications of drone swarms. For example, the Ziyan Blowfish vertical take-off and landing (VTOL) drone is one of several Chinese unmanned systems that market "intelligent swarming" capabilities, and was featured in a May 2019 YouTube video. In October 2002, state-owned enterprise China Electronics and Technology Group Corporation demonstrated the capability to launch swarms of dozens of "suicide drones" designed to overwhelm enemy defenses. *Source:* DARPA illustration. https://www.darpa.mil/program/gremlins

> this activity is to "[change] the structure of the global political system, forcing other nations to accept and adjust to China's new disposition."[18]

China's continued development of uncrewed aerial, surface, and even undersea vehicles—and, especially, its focus on swarms of uncrewed vehicles—is also notable.

The focus on drone swarms is an indicator of the attention PLA modernization is giving to moving toward "intelligentized" warfare, in which AI is more fully integrated into military activities at the tactical, operational, and strategic levels, in order to keep up with the increasing volume and velocity of salient information available to operators and decision-makers.

Swarms and autonomous systems offer one solution to dealing with the need for speedy decision-making, especially at the tactical level. Increasingly, though, PLA military thinkers are looking to AI as a tool to support humans and relieve the cognitive burden facing human operators and decision-makers, according to Elsa Kania, a noted China military-technology expert and adjunct fellow at the Center for New American Security.[19]

Kania notes in a recent essay published in National Defense University's *Prism* magazine that China is turning to hybrid intelligence and "brain-machine fusion" as one component of the push toward "intelligentization."[20] Citing He Fuchu, the respected former vice president of China's Academy of Military Sciences, Kania observes that some

18 Ibid.

19 Elsa B. Kania, "Minds at War: China's Pursuit of Military Advantage through Cognitive Science and Biotechnology," *Prism 8-3*, National Defense University Press, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

20 Ibid.

in the PLA see not just an expansion of conflict beyond the physical domain, but also a merging of digital, physical, and cognitive conflict, thereby providing new areas of military-technological competition between China and the United States, as well as other allies and partners.

> "In future conflict, the battlefield is expected to extend into new virtual domains. According to He Fuchu, 'The sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness (意识域); the human brain will become a new combat space.' Consequently, success on the future battlefield will require achieving not only 'biological dominance' (制生权) but also 'mental/cognitive dominance' (制脑权) and 'intelligence dominance' (制智权)."[21]

China's focus on dominating both informatized and intelligentized environments, and its impressive progress in evolving strike technologies such as drone swarms and hypersonic missiles, underscore the continued importance of the doctrine of military-civil fusion (MCF) in driving the PLA modernization effort. This doctrine enables the transfer of technology and know-how between China's commercial high-tech industry and applied-research institutes, on the one hand, and the PLA and supporting defense-industrial base on the other.

According to the US Department of State, "under MCF, the [Chinese Communist Party (CCP)] is acquiring the intellectual property, key research, and technological advances of the world's citizens, researchers, scholars, and private industry in order to advance the CCP's military aims."[22]

MCF is not a new concept, but it has become a bigger priority under President Xi Jinping. A Chinese Communist Party communique issued on October 29, 2020, said that a key target during the 14th Five-Year Plan (FYP) made several mentions of a requirement during the 14th FYP to deepen connections between commercial and military technologies.[23]

Jon Grevatt, Janes' Asia-Pacific industry reporter, believes that, especially in the wake of the growing regional and international pushback on some of China's behaviors, there will be even more of an effort "to deepen MCF to further

Representative Examples of Regional Responses to China's Military Modernization

China's military modernization has directly stimulated new investments and research, among Quad states in particular, in order to effectively deter China and be prepared to respond to crises and conflict in the region.

Australia's "2020 Defence Strategic Update" and "2020 Force Structure Plan" commit to spending $575 billion in total funding for defense over the next decade, which includes $270 billion in investment spending—the combination of procurement and research, development, testing, and evaluation budgets. Key technology and capability priorities include remotely piloted and autonomous uncrewed systems, directed-energy weapons, high-speed missile systems to deter China, and technologies that can ensure space resilience.[1]

In response to perceptions that China is considerably ahead in efforts to exploit the 4IR-enabled revolution in military affairs, the Indian Army commissioned a study in August 2020 to examine "niche and disruptive warfare technologies."

The study will include analysis of an extensive list of general technology areas such as AI, big-data analysis, blockchain, the Internet of Things, augmented and virtual reality, additive manufacturing, remotely piloted unmanned aerial systems, additive manufacturing, and quantum computing. It will also focus on specific capability areas, such as drone swarms, algorithmic warfare, hypersonic-enabled long-range precision-firing systems, directed-energy weapons, and loitering and smart munitions.[2]

1 2020 Force Structure Plan," Australian Department of Defense, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

2 "Amid LAC face off, Indian Army to conduct study on lasers, robotics, and AI for warfare", *Times of India,* August 8, 2020, https://timesofindia.indiatimes.com/india/amid-lac-face-off-army-to-study-lasers-robotics-ai-for-warfare/articleshow/77425169.cms

21 Ibid.

22 "The Chinese Communist Party's Military-Civil Fusion Policy; Fact Sheet," US Department of State, https://www.state.gov/military-civil-fusion/.

23 Jon Grevatt, "China to Deepen 'Civil-Military Fusion' in 14th Five Year Plan," *Janes*, November 2, 2020, https://www.janes.com/defence-news/news-detail/china-to-deepen-civil-military-fusion-in-14th-five-year-plan#:~:text=A%20communique%20issued%20on%2029%20October%20by%20the,prioritised%20deeper%20civilian-military%20integration%20during%20its%202021%E2%80%9325%20plan.

develop sophisticated applications of disruptive commercial technologies such as quantum computing, materials science, and AI in order to change the status quo."[24]

And, China's focus on MCF and deepening integration between commercial and military technology development activities is, at least partially, behind efforts in states across the region to create new structures and mechanisms for engagement with the commercial high-tech sector. For example, India, which is generally considered to have fallen behind China and other states in terms of its capacity to develop novel and disruptive 4IR technologies, has taken several important steps in 2020 to stimulate not just its organic defense-industrial base, but also the broader innovation community. Over the course of 2020, the Indian Ministry of Defence (MoD) launched the Innovation for Defense Excellence (iDEX) program to facilitate rapid development of new, indigenized, and innovative technologies for the Indian defense sector, and has also announced the establishment of eight advanced-technology centers to carry out research "on futuristic military applications and to support academia in efforts to undertake research on new technologies for military use."[25]

Beyond China: An Expanding Threat Spectrum and Gray-Zone Contingencies

Perceptions of strategic threat across the region are broader than just China. These concerns are intensifying and expanding, even if all states in the region do not view each of these threats the same way, or with the same urgency.

For example, North Korea's missiles are of general concern throughout the region, but especially for Japan, given its proximity to the Korean Peninsula and the history of North Korean test launches that directly threaten Japanese territory. Japan's perception of its security, and of its technology-development priorities, is also influenced by domestic factors, particularly demographic challenges such as an aging population and declining birth rate that will likely increase Japan Self-Defense Force (JSDF) demand for unmanned systems.

Similarly, the 2019 national security strategy for India released by the Congress Party, which offers a thorough outline of Indian national security concerns, stresses a different set of challenges—namely its contested boundaries with both Pakistan and China as well as extremism and internal security. In fact, the document's primary discussion of disruptive technology is focused on the deleterious societal impacts, labor displacement, and widening disparities in wealth and economic security that widespread adoption of AI and robotics could create.[26]

Nontraditional and human security concerns are also becoming a bigger priority across the region, including for China. The CCP State Council's "China's National Defense in the New Era" white paper, published in July 2019—five months before the start of the outbreak of the coronavirus in China—presciently observed that "the threat of non-traditional security issues posed by natural disasters and major epidemics is on the rise." [27]

Concern about these nontraditional security and defense challenges has been amplified by the coronavirus pandemic, which has expanded and reordered priority missions for defense and security communities in the region as well. As the Australian "Defence Strategic Update" notes, "threats to human security, such as the coronavirus pandemic and natural disaster, mean disaster response and resilience measures demand a higher priority in Defence planning."[28]

Gray-Zone Contingencies

Defense technology and capability priorities are also being shaped by the prevalence and continued potential for gray-zone contingencies.

These contingencies involve largely state or state-backed actions that leverage military, political, social, economic, and commercial technological means to change the status quo in ways that are below the threshold that would typically lead to a military response. A recent RAND report further characterized gray-zone contingencies as blurring the line between military and nonmilitary actions.[29]

The range of specific gray-zone-type situations may be bound only by the limits of the imagination of clever political and military strategists and scenario planners. A 2020

24 Phone interview with Jon Grevatt, October 20, 2020.

25 "Innovations for Defence Excellence: Operationalization Plan for Defence Innovation Organization (DIO) and Defence Innovation Fund (DIF)," Innovations for Defence Excellence, https://idex.gov.in/documents/5d5fc494b6d68d7ae502f7f3_Complete-document-on-iDEX_1.pdf; "DRDO Sets Up 8 Tech Centers for Research on Futuristic Military Applications," *Times of India*, September 19, 2020, https://timesofindia.indiatimes.com/india/drdo-sets-up-8-tech-centres-for-research-on-futuristic-military-applications/articleshow/78204834.cms.

26 "India's National Security Strategy," India Congress Manifesto, March 2019, https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf.

27 "China's National Defense In The New Era (新时代的中国国防)," PRC State Council, July 24, 2019, http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

28 "2020 Defence Strategic Update."

29 Lyle J. Morris, et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War, RAND*, 2019, https://www.rand.org/pubs/research_reports/RR2942.html. Also available in print form.

report from defense contractor QinetQ on the potential of technologies to deal with these challenges describes five categories of gray-zone contingencies, including[30]

- deniable attacks;
- information operations;
- use of proxy forces;
- economic coercion; and
- territorial encroachment.

Each of these categories is either playing out now or has already played out in the Indo-Pacific, both independently and in combination with one another. The QinetQ report references China's island building in the South China Sea as an example of a territorial-encroachment scenario, but one could also argue that the use of China's Maritime Militia to surveil and intimidate foreign military and commercial vessels constitutes use of proxy forces, and a form of economic coercion as well.[31]

Across these disparate categories—or others that other observers can envision—at least three important commonalities exist that are influencing technology investment and organizational priorities in the region.

First, the specific threats captured by these categories are frequently difficult to detect and attribute, much less actually anticipate, thereby placing a premium on technological innovation to support greatly enhanced situational awareness and, to a lesser extent, deterrence and dissuasion.

Second, gray-zone threats can place pressure not just on traditional military and security forces, but also on many aspects of government, society, and the commercial sector, once again broadening concepts of national defense. As a result, governments in the Indo-Pacific are not just investing in means to detect and deter subtle threats, but also in building vigilance among the population and private sector.

Singapore's "Total Defence" concept stands out as a useful example, but it is not the only one across the region.[32] Actions outlined in "Australia's Cyber Security Strategy 2020" include highly tactical measures to engage communities, companies, and even families as a means of "improving community awareness of cyber security threats," providing "advice for small and medium enterprises to increase their cyber resilience" and deliver "clear guidance for businesses and consumers about security Internet of Things devices."[33]

Third, gray-zone situations also tend to require rapid, proactive, and focused responses that thread the needle of forcefully reestablishing a challenged status quo without needlessly escalating to a more dangerous situation. While there is certainly room for kinetic responses (or at least the credible threat of the use of kinetic force) to gray-zone situations, defense communities are also investing in non-kinetic capabilities such as "soft-kill" directed-energy counter-drone technologies, personal protection equipment, electronic attack, and the ability to effectively compete in the cyber and information domains. As the

Singapore's "Total Defence" Concept and the Blurring of Military and Non-Military Challenges to National Defense

Singapore's six-pillar strategy of Total Defence is a useful example of the way in which defense communities in the Indo-Pacific are being forced to consider and prepare for "the way that war is conducted today" and to respond to "all forms of attack, both military and non-military."

While the strategy dates back to 1984, it has been updated in recent years to reflect the range of new challenges the city-state now faces, including those "from the digital domain that have no physical boundaries or battlefields" in addition to terrorism, disease, and economic disruptions.

The first three pillars of Total Defence revolve around traditional concepts of military defense, civil defense, and economic defense. The strategy also emphasizes more modern concepts of social defense, digital defense, and psychological defense, in order to better protect Singapore and its citizens from disinformation, cyberattacks, and other creative attempts to undermine the country's will to fight or respond to pressing challenges to national or human security.

30 "Confidence in Chaos: How to Use Emerging Technologies to Combat Grey Zone Threats," QinetQ, https://www.qinetiq.com/en-us/insights/grey-zone-warfare.

31 Ibid.

32 "Total Defence Information Page," Singapore Civil Defence Force, https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence. This is also the source for quotes and information in the "Total Defence" text box.

33 "Australian Cyber Security Strategy 2020," Australian Department of Home Affairs, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Australian "2020 Defence Strategic Update" summarized, the most important requirements for meeting gray-zone challenges are "improved situational awareness, electronic warfare and information operations."[34]

The "New" Domains of Warfare: Space, Cyber, and Electromagnetic

Activity and competition is intensifying in and across what the "Defense of Japan 2020" paper refers to as the three "new domains" of space, cyber, and the electromagnetic spectrum.[35]

These three domains are crucial to the future of military conflict. However, the "Defense of Japan 2020" paper makes clear that these three domains are also equally as important to "everyday life" and other civil and commercial purposes, further underscoring the merging of explicitly military and nonmilitary threats to national and regional security in the Indo-Pacific.[36]

Space

Barriers to commercial and military activity in space have reduced over the last decade, allowing more commercial and government actors to pursue space-related or space-based programs and initiatives. According to the *Diplomat's* Rajeswari Pillai Rajagopalan, "costs are coming down, technological hurdles are lower, and new space collaboration and partnerships driven by geopolitical goals" are serving to democratize the domain.[37]

The democratization of military space is certainly under way as the need to connect people, platforms, and systems across multiple domains increases in an informatized operating environment. More states are developing and deploying space-based C4ISR capabilities and the counterspace capabilities that can place surveillance and communications satellites at risk. Australia's "2020 Force Structure Plan" captures the importance of space for modern militaries, assessing that "space capabilities provide situational awareness and the delivery of real-time communications and position, navigation and timing information, essential for 21st century military operations."[38]

Militaries have also begun to organize around the domain, especially in the Indo-Pacific, where China, the United States, India, and, most recently, Japan, have consolidated military space activities to increase integration, collaboration, and coordination among different military and civilian government agencies supporting military space missions.

Table 1: Organizations focused on military operations in space recently established by Indo-Pacific actors.

Country	Defense Space Agency
People's Republic of China (PRC)	PLA Strategic Support Force (PLASSF) (2015)
United States	Space Force (2019)
India	Defense Space Organisation (2019)
Japan	Space Operations Squadron (2020)

Military space is a clear priority for China's military modernization, and the PLA views outer space—along with cyber—as "a commanding height in international strategic competition."[39] The Secure World Foundation's 2020 report on global counterspace capabilities also emphasizes the importance of space to China's A2/AD strategy and military operations, observing that "military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance."[40]

China's PLA-run space program has made impressive strides in recent years, including the establishment of the

34 "2020 Defence Strategic Update."

35 "Defense of Japan 2020," *New Domains*, Ministry of Defense, 2020, https://www.mod.go.jp/e/publ/w_paper/wp2020/pdf/index.html.

36 Ibid.

37 Rajeswari Pillai Rajagopalan, "Managing New Actors in the Space Domain," *Diplomat*, June 29, 2019, https://thediplomat.com/2019/06/managing-new-actors-in-the-space-domain/.

38 "2020 Force Structure Plan," Australian Department of Defense, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

39 "China's Military Strategy," State Council, People's Republic of China, May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

40 Brian Weeden and Victoria Samson, "Global Counterspace Capability: An Open Source Assessment," Secure World Foundation, April 2020, https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

On March 27, 2019, India's Defence Research and Development Organisation (DRDO) successfully launched the Ballistic Missile Defence (BMD) Interceptor missile in an anti-satellite (ASAT) missile test entitled 'Mission Shakti.' This missile engaged an Indian orbiting target satellite in low-Earth orbit (LEO) in a 'Hit to Kill' mode, and was launched from the Dr. A.P.J. Abdul Kalam Island in Odisha. *Source:* Indian Ministry of Defence, Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Launch_of_DRDO%27s_Ballistic_Missile_Defence_interceptor_missile_for_an_ASAT_test_on_27_March_2019.jpg

People's Liberation Army Strategic Support Force (PLASSF) in 2015 and the launching of the twenty-seventh and final satellite associated with the dual-use Beidou Global Navigation Satellite System (GNSS) earlier this year.[41] It has also achieved milestones related to the development of several types of Long March rockets, as well as novel C4ISR satellite payloads.[42]

But, perhaps most importantly to regional defense-technological capability investments, China has continued to advance its counterspace capabilities. These capabilities range from inelegant and easily detectable direct-ascent anti-satellite missiles to more subtle means of disabling or degrading space-based communications and ISR, such as directed energy to "dazzle" or blind satellites, co-orbital or even kamikaze satellites designed to disable adversary satellites, or cyberattacks on satellite communications.[43]

In part due to China's emphasis on space, but also due to other strategic and geopolitical concerns, the United States' Quad partners—among other states in the region—have

41 Andrew Jones, "China Launches Final Satellite to Complete Beidou System, Booster Falls Downrange," *Space News*, June 23, 2020, https://spacenews.com/china-launches-final-satellite-to-complete-beidou-system-booster-falls-downrange/#:~:text=The%20new%20satellite%20will%20complete,for%20testing%20and%20domestic%20services.

42 "China launchers heaviest satellite to test key technologies", *Xinhua Net*, December 27, 2019, http://www.xinhuanet.com/english/2019-12/27/c_138662080.htm

43 Tate Nurkin, et al., "China's Advanced Weapons Systems," US-China Economic and Security Review Commission, May 2018, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf.

greatly enhanced their focus on military space in the last two years.

Japan has been particularly assertive in introducing new capabilities and aligning its organizational structure to account for the growing importance of space for both military and civil/commercial activities. In February 2020, Japan successfully launched its eighth ISR satellite into orbit. The satellite was ostensibly launched to observe North Korea's missile activities, though it will likely serve a broader purpose in tracking security threats across Northeast Asia. Japan currently has stated plans for two more ISR satellites.[44]

On May 18, Japanese Defense Minister Taro Kono officially inaugurated Japan's Space Operations Squadron. The organization's main mission is to protect Japanese (and American) satellites by operating a space-surveillance system designed to track space debris and the position of other satellites, in order to avoid collision or malicious counterspace threats.[45]

Collaboration with the United States has been, and continues to be, a key component of Japan's military space efforts. A 2019 agreement aims to link the space-situational-awareness (SSA) systems of Japan's Self-Defense Forces (JSDF) and the US military by 2023. The SSA system will share real-time information on threats to both Japanese and US satellites from third-country threats and space debris.

Australia's "2020 Force Structure Plan"—released alongside the "2020 Defence Strategic Update"—includes a section on Australia's planned space investments. The Department of Defence plans to invest approximately $7 billion over the next decade to "improve the resilience and self-reliance of Defence's space capabilities and enhance a large number of space-dependent capabilities, including communications satellites and ground control stations that will be under sovereign Australian control."[46]

This focus on space is reflected in the country's stated defense science and technology priorities. One of the eight high-impact technology "Star Shots" laid out in the "Defense Science and Technology Strategy 2030" is to build "a resilient multi-mission space capability that can provide resilient global communications, position, navigation, and timing (PNT), and geospatial intelligence (GEOINT) capabilities direct to ADF users, enabled by a low earth orbit SmartSat constellation."[47]

China's existing and emerging counterspace capabilities have also served as a catalyst for India's military space program, which experienced an active 2019. On March 27, 2019, India's Defense Research and Development Organization (DRDO) revealed that it had successfully tested a direct-ascent anti-satellite (ASAT) weapon by shooting an aging satellite out of low-Earth orbit (LEO), about three hundred kilometers above Earth.[48] The test was seen as an effort to enhance and demonstrate India's space deterrence capabilities, and was quickly followed in April 2019 by the announcement of the establishment of the tri-service/joint Defence Space Agency, and in June 2019 by the holding of the IndSpaceEx tabletop wargame that sought to identify vulnerabilities in India's space security.

Cyber

The cyber domain is also a preoccupation of defense and security communities as competition and conflict between states, and between state and non-state actors, manifest in the information domain and social media.

At an operational military level, the contest in the cyber domain has intensified as reliance on information and communications technologies for command and control, among other functions, has increased. It is worth remembering that China's 2015 defense white paper included both space *and cyber* as the commanding heights of emerging strategic competition.

The ability of a state or non-state actor to take over, spoof, degrade, or deny access to these networks, or to be able to steal personal information that could affect individual decision-making or technological data that could provide a military-technological advantage, all could have grave implications for military operations and military-technological competition.

Responding to the cyber threat requires technical innovation. But, just as with space, it also requires new ways of

44 Gabriel Dominguez, "Japan Launches Another IGS Reconnaissance Satellite," *Janes Defence Weekly*, February 11, 2020, https://customer.janes.com/Janes/Display/FG_2697701-JDW.

45 Kosuke Takahashi, "Japan Sets Up Its First 'Space Operations Squadron,'" *Janes Defence Weekly*, May 18, 2020, https://customer.janes.com/Janes/Display/FG_2849229-JDW.

46 "2020 Force Structure Plan," Australian Department of Defense, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

47 "More, Together: Defence Science and Technology Strategy 2030."

48 Doris Elin Urrutia, "India's ASAT Test Is A Big Deal. Here's Why," *Space.com*, March 19, 2019, https://www.space.com/india-anti-satellite-test-significance.html.

thinking about the domain and then organizing to better marshal and integrate human and physical resources to defend military, commercial, civilian-government, and critical-infrastructure networks. Accordingly, many of the most visible indicators of regional defense community activity in the otherwise opaque cyber domain are seen in the release of national plans and the trend of new cyber-focused organizations in Indo-Pacific militaries. India, Australia, and Singapore have all established defense organizations dedicated to cyber operations since 2018.

Concepts of cybersecurity are also being expanded in the region to include the deleterious strategic consequences of information, influence, and disinformation campaigns that, according to the Indian National Security Strategy released by the Congress Party, "hostile and inimical powers" are using to "sow discord amongst people, spread propaganda and weaken faith in government."[49]

China's efforts to use Western and Chinese-language social media to further influence operations and disinformation campaigns have become more prominent and, for Quad states and others in the region, worrying. Oxford University's Computational Propaganda Project's "The Global Disinformation Order 2019" determines that "China has become a major player in the global disinformation order" that has moved from solely using domestic social media platforms to also aggressively using US platforms such as Twitter, Facebook, and YouTube."[50]

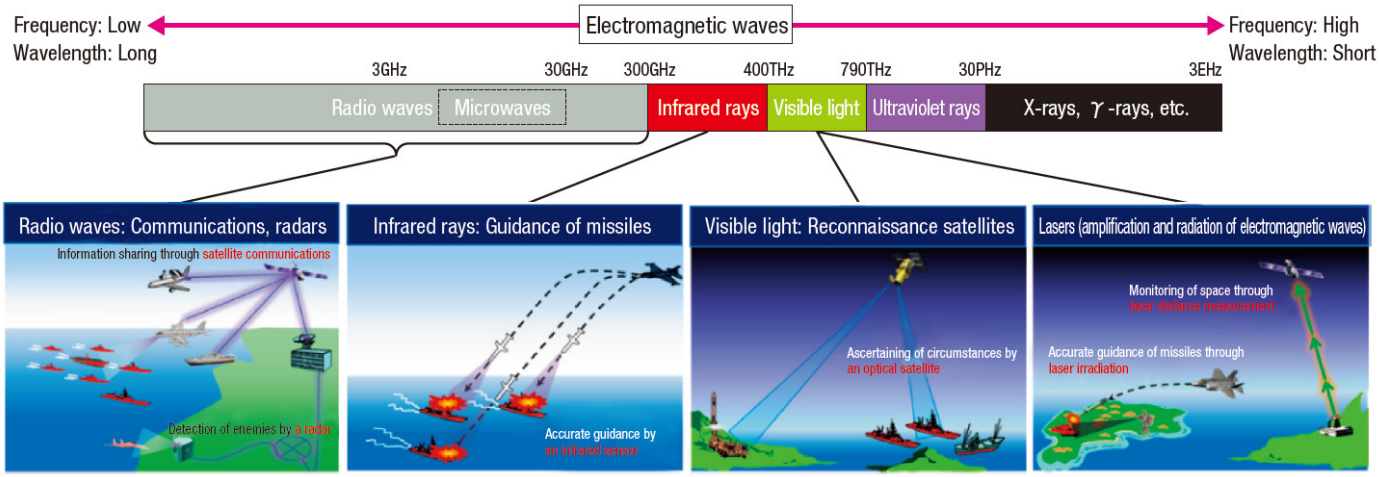
Electromagnetic Spectrum

The EM domain and electronic warfare (EW) are closely related to both the cyber and space domains and serve as a crucial medium for most command, control, and communication equipment, as well as radar systems.

EW—to include electronic attack, electronic defense, and electronic support—is a crucial priority for militaries across the Indo-Pacific. As the "Defense of Japan 2020" paper points out, "securing superiority in the electromagnetic domain is indispensable for modern operations."[51]

China has moved quickly in the development of EW capabilities, given the importance China's modernization effort has placed on information dominance and the need to asymmetrically target US and allied C4ISR capabilities.

But, other states have also focused investment on EW capabilities. In 2020, the JSDF revealed the establishment of three new EW units, including an announcement in September that the Japan Ground Self Defense Force (JGSDF) will activate a new EW unit in the Okinawa



The electromagnetic spectrum is an increasingly important domain of warfare. This graphic from the "Defense of Japan 2020" paper demonstrates how electromagnetic waves of different frequencies and wavelengths can be used in a variety of missions and military applications. *Source:* Japan Ministry of Defense. https://www.mod.go.jp/e/publ/w_paper/

49 "India's National Security Strategy."

50 Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," Oxford University Computational Propaganda Research Project, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

51 "Defense of Japan 2020."

Prefecture in the far south of Japan's archipelago, proximate to the contested Senkaku Islands. Previously, the JGSDF had disclosed in June that the Amphibious Rapid Deployment Brigade had activated an organic EW unit, and earlier in 2020 announced the 1st EW Unit, an independent formation containing three companies based on the northern island of Hokkaido. All of these units are expected to be activated by 2025.[52]

Dr. Thomas Withington, an EW specialist, sees these moves in the context of a changing EW environment in the Indo-Pacific.

According to him, there is a pressing need across the region to "move from tactical EW to operational EW"; that is, moving away from emphasis on "platform protection to actually fighting and prevailing in the electromagnetic spectrum especially in operational environments that stress joint and multi-domain operations."[53]

Critical to this transition will be investments not only in electronic attack capabilities, but also in electronic support—the sort of capabilities that allow militaries to exploit the data they collect and the novel capabilities they develop: data analysis, emitter classification, signals-intelligence (SIGINT) analysis, and information management and distribution tools, as well as training. According to Withington, Australia stands out as having invested in this "back office" aspect of EW, but across the region more needs to be done to be able to exploit signals intelligence collection, electronic support and platform-protection activities.[54]

The Blurring of Domains and Multi-Domain Operations

As activity in space, cyberspace, and the EM spectrum becomes more sophisticated, distinctions between these domains are blurring.

Dr. Withington observes that while EW, information operations, space and counterspace, and cyber operations all retain specific distinct characteristics, operations in these domains "are definitely converging." One representative example: electronic attack is more and more serving as a "vector" to inject malicious code to exploit and disrupt adversary command-and-control networks, or as part of information operations to agitate elements of competitor or adversary populations.[55]

Multi-Domain Operations: Fusing the "Old" and "New"

Modern military operations are increasingly taking place not just in individual and isolated domains, but also across the traditional domains of land, air, and sea, as well as space, cyberspace, and the EM spectrum.

Coordinating operations across these domains—for example, by using the EM spectrum, space, and cyberspace to communicate to platforms, systems, and personnel in the traditional domains, or to deter and defeat EW operations—has become a central priority of modern militaries across the Indo-Pacific and throughout the world.

According to "The Defense of Japan 2020," "operations that organically fuse capabilities in the new domains and traditional domains of land, sea, and air to exercise domain-crossing capabilities have thus become vitally important."

The blurring of the lines separating these domains is shaping future technology and capability priorities, but, once again, it is also shaping the way militaries across the region organize. As noted above, the PLA announced the formulation of the PLASSF in December 2015, demonstrating the holistic way in which the PLA views these capability areas, to include psychological-warfare and disinformation operations.

North Korea has also combined its EW capabilities with significant components of its cyber activities.

In a comprehensive July 2020 report entitled "North Korean Tactics," the US Army lays out a detailed view of how the North Korean military has integrated EW, cyber, and psychological warfare operations into a single organizational unit known as the Electronic Warfare Bureau. Three of the bureau's four units are focused on cybersecurity tasks, especially gathering intelligence on vulnerabilities in enemy computer networks, performing financial cybercrime, and attacking adversary computer networks.

52 Dr. Thomas Withington, "More EW Units for Japan's Army," *Armada International*, September 25, 2020, https://armadainternational.com/2020/09/more-ew-units-for-japans-army/.

53 Phone interview with Dr. Thomas Withington, October 13, 2020.

54 Ibid.

55 Ibid.

The fourth unit is a more explicit and traditional EW unit known as the EW Jamming Regiment, again highlighting the intersection between the cyber and EM domains.[56]

III. Capturing and Monitoring Technological Innovation: The Five Revolutions[57]

Defense communities across the Indo-Pacific are turning to investment in new and emerging dual-use 4IR technologies to better cope with the complex, uncertain, and fast-moving strategic context and expanding threat environment described above.

The identity of the specific technologies of interest is not a secret. A survey of government documents from India, China, the United States, Australia, and Japan, and of open-source reporting and commentary about each country's defense-technology development priorities, reflects widespread and overlapping interest in the technologies in Table 2 below.

These lists are useful, but they are also vague. They tend to capture *categories* of technologies—AI, advanced materials, energy capture, and storage are all useful examples—that include multiple specific technologies or techniques. Many of the technologies of common interest have an array of applications—for instance, blockchain, unmanned systems, or directed energy—that can support a number of missions and achieve various effects. Moreover, different states will have different resources available for developing these technologies for military use.

In fairness, some militaries are more open and granular in their discussion of their interest in emerging technologies and their objectives in developing them. Australia's "Defence Science and Technology Strategy 2030" includes a robust discussion of the technological context and landscape, but also establishes eight high-impact "Star Shot" initiatives that help observers understand where its technological investment priorities rest, including[58]

- resilient multi-mission space;
- information warfare;
- agile command and control;
- quantum-assured position, navigation, and timing;
- disruptive weapon effects;
- operating in chemical, biological, radiological, and nuclear (CBRN) environments;
- battle-ready platforms; and
- remote undersea surveillance.

Still, the task of capturing and assessing the strategic and operational impact of defense innovation efforts based on monitoring technologies can be overwhelming, and can leave analysts and decision-makers with an incomplete understanding of how technology is shaping the future of military capabilities, the threat environment, and strategic competition in the Indo-Pacific.

Table 2: A list of technologies of general interest to militaries in the Indo-Pacific.

Artificial intelligence	5G networks	Quantum computing and encryption
Additive manufacturing	Unmanned systems and robotics	Hypersonic flight
Advanced materials	New energy capture, storage, and distribution	Directed energy
Electromagnetic weapons	Secure communications	Neuro and biotechnologies
Internet of Things	Augmented and virtual reality	Big-data analysis
Cloud computing	Blockchain	Smart sensors
Space technologies		

56 Dr. Thomas Withington, "Know Your Enemy," *Armada International*, August 27, 2020, https://armadainternational.com/2020/08/know-your-enemy/.

57 The author developed this framework while at IHS Jane's (now Janes) in 2016. It originally featured four revolutions, and the content was first published as part of the Eurosatory Show Daily in 2016. The author has briefed versions of the framework in both public and private settings over the last four years. The framework has been refined and expanded to include cyber and information operations in 2019 and 2020.

58 "More, Together: Defence Science and Technology Strategy 2030."

Figure 1: The Five Revolutions in capabilities that militaries seek to achieve through technological innovation and development (source: Tate Nurkin, with images from Microsoft 365).

A more constructive and efficient approach is to focus instead on the *effects* that defense communities are trying to achieve through their research and development (R&D) efforts and through associated organizational changes and industry-engagement efforts.

Here, most modern militaries are remarkably consistent in the outcomes they are trying to achieve, namely driving step-changes—or "revolutions"—in capabilities in five broad areas.

Like all frameworks, this one comes with caveats. The seams between these five revolutions are not always clean. Broad capability areas such as human-machine teaming—and especially brain-machine interfaces—could fall into both the first and second revolutions, and possibly the fourth. Components of EW could also easily be disentangled and captured by perception, processing, and cognition (SIGINT collection and analysis); human and machine performance (electronic defense); and communication, navigation, targeting, and strike (electronic attack).

Even with room to debate how some capabilities might be categorized, in an environment in which technologies and domains are blurring and fusing into an amorphous, sometimes difficult to disaggregate mess of "innovation" and "multi-domain operations," there remains utility in understanding what effects militaries are trying to achieve through their investment in emerging technologies.

1. Toward Perfect Situational Awareness: A Revolution in Perception, Processing, and Cognition

Decision-makers and operators are under considerable pressure to speed up Colonel John Boyd's OODA (observe-orient-decide-act) loop to, in the words of the Australian Defence Science and Technology Strategy 2030, "understand, shape and dominate the future multi-domain battlespace."[59]

This revolution concentrates on efforts to accelerate the first three components of the loop—observe, orient, and decide—by improving the scale of information collected, the pace of its processing, and, as a result, the quality of situational awareness on which decisions are made and subsequent actions taken.

Novel capabilities, such as smart-sensor networks, persistent and frequently uncrewed ISR systems, AI-enabled

59 Ibid.

radio-image identification technology (a priority application of AI for Japan's Self-Defense Force), and even more aspirational capabilities such as synthetic-biology anti-submarine warfare sensors are all among the broad suite of technology-enabled capabilities designed to collect more, more frequent, and more accurate information.

The perception, processing, and cognition revolution is particularly important in the Indo-Pacific context, which is marked by massive distances, different topographies, long borders and boundaries, large and crowded cities, and a strong maritime nature.

Being able to persistently collect data in contested urban environments across huge geographical spaces and in opaque environments, such as the undersea domain, is essential to first detecting, and then rapidly devising responses to, fast-moving, if distant, challenges. As noted above, Australia has prioritized enhancing remote undersea sensing.[60] In addition, DARPA's "Ocean of Things" project aims to "seed the seas with thousands of floating sensors, monitoring everything that passes from aircraft to submarines."[61]

The processing and cognition component of this revolution is also relevant because, while the distances across the region can be vast, the speed at which platforms, systems, and sub-threshold threats move has eroded one of the values of the region's strategic geography: time to react. Mark O'Neill of Australia's Lowy Institute argues in a recent article that "geography, previously a useful strategic advantage for island nations, is less of an asset when facing 21s century technologies that are agnostic about distance and domain."[62] AI and big-data technologies that enable information and intelligence to be processed quickly, detect patterns and anomalies, and better understand the nature of operational and tactical environments will buttress efforts to craft effective responses along compressed timelines.

Focus Areas of the Human and Platform Performance Revolution in the Indo-Pacific

- Training and simulation
- Human performance enhancement and hyper-enabled operators
- Exoskeletons
- Brain-machine interfaces and other types of human-machine teaming
- New energy capture and storage and design approaches to enhance endurance and efficiency
- New lightweight, dynamic, and programmable materials
- Active protection systems
- Electronic defense
- Enabling operations in CBRN environments

2. An Age of Hyper-Enabled Platforms and People: A Revolution in Human and Machine Performance

The human and machine performance revolution calls upon 4IR technologies and novel materials to optimize the performance of people, platforms, and systems. Of particular interest is the ability of technologies to improve a suite of common attributes that are vital for the future effectiveness of people and machines, including

- health and recovery capacity;
- speed, strength, and maneuverability;
- power storage and endurance/persistence;
- protection and survivability, including in harsh environments;
- adaptability and resilience;
- connectivity;
- vision, detection, and cognitive capacity; and
- human-machine teaming.

For platforms and some uncrewed systems, this revolution centers on dynamic materials that suppress electromagnetic emissions or enhance kinetic protection. It also features active protection systems that offer proactive defense for crewed platforms against a range of mainly kinetic threats.

Design approaches such as biomimicry are also relevant to ensuring survivability, endurance, and stealth of unmanned systems, depending on the context. In May 2019, South Korea's Defense Acquisition Program Administration (DAPA) announced it is pursuing the development of biomimetic robot systems designed to mirror the natural movements of animals and insects, with plans to field these systems as early as 2024. According to DAPA spokesman Park Jeong-eun, "Biometric robots will be a game changer in

60 "More, Together: Defence Science and Technology Strategy 2030."

61 David Hambling, "DARPA Progress With 'Ocean of Things' All-Seeing Eye On The High Seas," *Forbes*, August 13, 2020, https://www.forbes.com/sites/davidhambling/2020/08/13/darpas-ocean-of-things-is-an-all-seeing-eye-on-the-high-seas/#35226caaf270.

62 Mark O'Neill, "Australia's New Strategic Geography," Lowy Institute, January 13, 2020, https://www.lowyinstitute.org/the-interpreter/australia-s-new-strategic-geography.

One of the US Army's eight cross-functional teams (CFTs) is dedicated to creating a synthetic training environment (STE) to improve soldier training. Here, US Army soldiers assigned to 10th Special Forces Group (Airborne) use and fire an M3E1 Multi-Role Anti-Armor Anti-Personnel Weapon System (also known as a Carl Gustav recoilless rifle) during a Reconfigurable Virtual Trainer demonstration at the 7th Army Training Command's Grafenwoehr training area, Germany, on February 13, 2020. *Source:* US Army photo by Markus Rauchenberger. https://www.dvidshub.net/image/6102694/carl-gustav-virtual-training-grafenwoehr

future warfare, and related technologies are expected to bring about great ripple effects throughout the defence industry."[63]

Multi-faceted efforts to develop "hyper-enabled human operators" are also an important part of this revolution, both within the US military and in several defense communities in the Indo-Pacific.[64]

Advancement in AI, virtual and augmented reality, cloud computing, haptics, and other associated technologies are facilitating more advanced and useful synthetic training environments. Virtual training environments reduce costs of training while simultaneously creating new opportunities for training "reps and steps" that will allow individuals and units to improve performance and better take advantage of more expensive—and, in the age of COVID-19, riskier—live training exercises.

AI is a particularly potent training technology that can enable dedicated virtual assistants, tailored training curricula, and more efficient mining of past training data, all of which can play a role in boosting human performance. Integrating machine and deep learning into wargames will also enhance the fidelity of simulations, which, in turn, can better prepare personnel for more complicated defense and

63 "South Korea to Develop Bio-Inspired Military Robots for Future Warfare," Yonhap News Agency, May 12, 2019, https://en.yna.co.kr/view/AEN20190510008000325.

64 Patrick Tucker, "Special Operations Command Made a Mind-Reading Kit For Elite Troops," *Defense One*, December 11, 2019, https://www.defenseone.com/technology/2019/12/specops-lab-made-mind-reading-kit-elite-troops/161830/.

security environments to include the subtle, difficult-to-detect, and frequently sensitive gray-zone contingencies prevalent in the Indo-Pacific strategic context.

A recent example of the flexibility and utility of virtual training environments is seen in the Royal Australian Air Force's (RAAF) Exercise Virtual Pitch Black. The exercise—held over two weeks in late June and early July 2020—allowed the RAAF to train virtually during heightened concerns about COVID-19.[65]

One of the key aspects of the exercise was the merging of simulators that existed separately, creating an integrated training system that delivered a complexity, density, and scale that effectively represented contested, degraded, and operationally limited environments. A spokesman for the Department of Defence noted at the conclusion of the exercise that "large-scale virtual exercises such as VPB20 are expected to increase in frequency and the RAAF, through the [Air Warfare Centre], is investing to create the Advanced Training and Test Environment (ATTE)."[66]

Development of technologies that facilitate a deeper connection between humans and machines, such as human-machine hybrids and brain-machine hybrids, are also gaining momentum, especially in the United States and China. In December 2019, the US Army released a report entitled "Cyber Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DoD." The report observes that ocular enhancements, optogenetic bodysuit sensor webs, exoskeletons, and auditory enhancements all have the potential to "incrementally enhance performance beyond the normal human baseline" for military operators while "the development of direct neural enhancements of the human brain for two-way data transfer would create a revolutionary advancement in future military capabilities."[67]

This effort to fuse human and machine intelligence and functionality is also a growing preoccupation of China's military and civilian R&D effort. A September 2020 report from the Center for Security and Emerging Technologies at Georgetown University argues that "China has engaged in a nationwide effort to 'merge' artificial and human intelligence as a major part of its next-generation AI development program" through multiple types of brain-machine interfaces.[68]

3. New Efficiencies and the Impending Design Age: A Revolution in Manufacturing, Supply Chains, and Logistics

Additive manufacturing, advanced automation, Internet of Things, digital design and testing, cloud manufacturing, and emerging manufacturing techniques like four-dimensional (4D) printing and synthetic biology manufacturing are combining to usher in a new industrial design age, in which manufacturing processes and material properties will be seen as powerful enablers of constructive innovations in capabilities, rather than as constraints.[69]

The USAF's September announcement of a digitally designed and developed next-generation aircraft has already provided indications of the revolutionary efficiencies in costs and timelines these technologies can generate. Another representative example is the incorporation of AI-enabled predictive maintenance to calculate the health of assets and identify trends in data, allowing militaries to greatly increase the efficiency of logistics and sustainment by anticipating potential failures and ensuring that vehicles stay in service for as long as possible.

Australia's Defence Science and Technology Organisation (DSTO) has included a holistic view of digital manufacturing and predictive maintenance as one of its eight "Star Shots" under the label of "battle-ready platforms." The concept incorporates data analytics, machine learning, and digital twinning to help "predict material state to guarantee platform availability and capability."[70]

The widespread introduction over the next decade of digital design, advanced manufacturing, and predictive-maintenance technologies will necessarily upend current logistics systems, industry dynamics, and industrial supply chains, creating layered challenges for defense communities and industry across the Indo-Pacific.

Most notably, point-of-use printing, digital design, and other technologies and applications will upset industry

65 Flight Lieutenant Bel Scott, "Seizing the Opportunity for Simulated Success," Australian Government, Department of Defence, July 16, 2020, https://news.defence.gov.au/capability/seizing-opportunity-simulated-success.

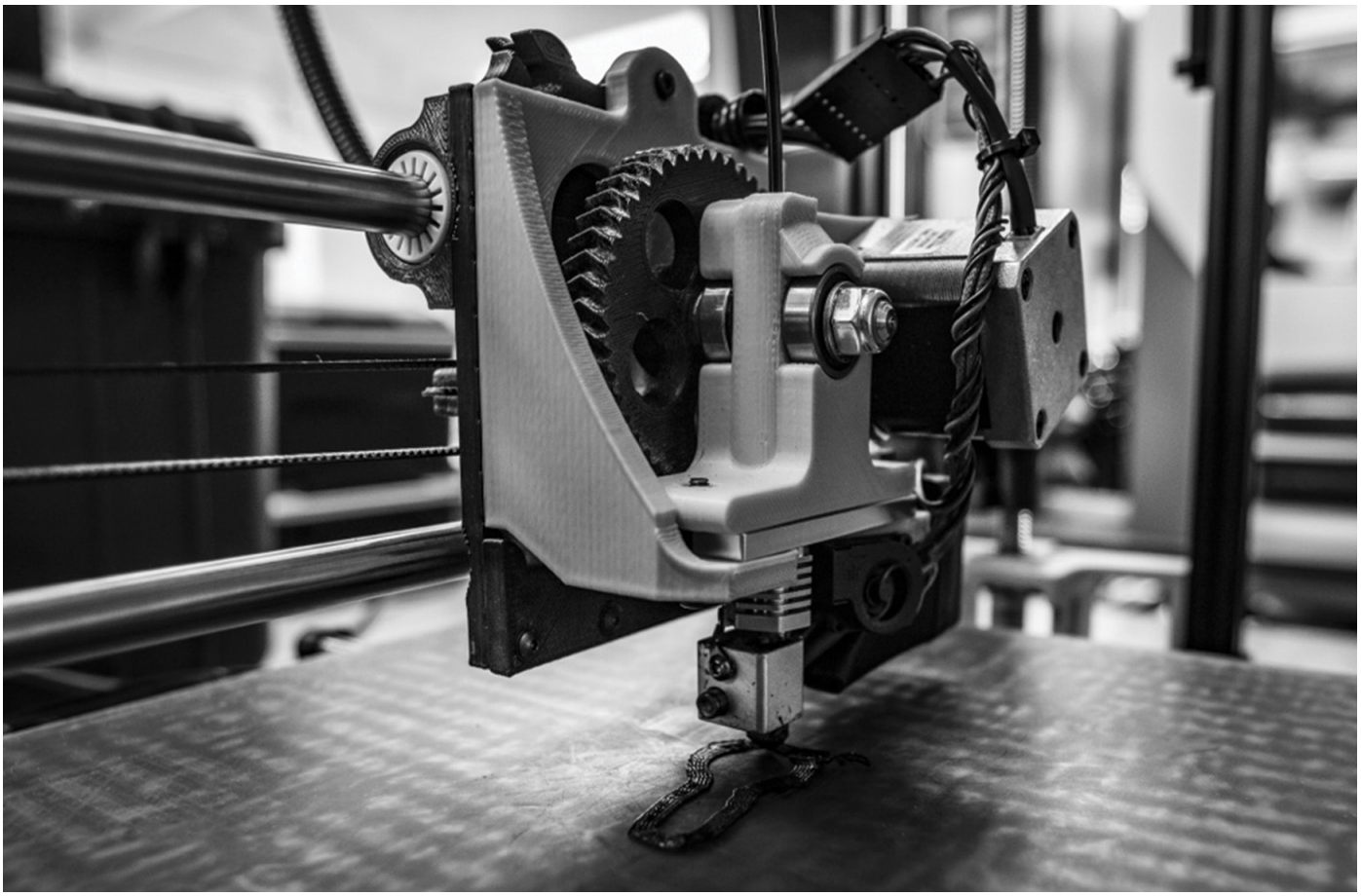
66 Mike Rajkumar, "Exercise Pitch Black 20 Goes Virtual for 2020," Halldale Group, August 18, 2020, https://www.halldale.com/articles/17468-exercise-pitch-black-20-goes-virtual-for-2020.

67 "Cyber Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DoD," U.S. Army, Biotechnologies for Health and Human Performance Council Study Group, November 2019, https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/300458.

68 William C. Hannas, et al., "China AI-Brain Research: Brain-Inspired AI, Connectomics, Brain-Computer Interfaces," Center for Security and Emerging Technology, Georgetown University, September 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-China-AI-Brain-Research.pdf.

69 Tate Nurkin, "Testimony before the US-China Economic and Security Review Commission Hearing on 'Implications of China's Military Modernization,'" in *Hearing on China's Military Reforms and Modernization: Implications for the United States*, February 15, 2018, https://www.uscc.gov/hearings/chinas-military-reforms-and-modernization-implications-united-states

70 "More, Together: Defence Science and Technology Strategy 2030."



The US Army's first 3D printer, operated by soldiers assigned to 194th Combat Sustainment Support Battalion, 2nd Sustainment Brigade, 520th Support Maintenance Company, manufactures an ignition switch for a Humvee at Camp Humphreys in the Republic of Korea on October 29, 2018. The printer uses the method of additive manufacturing, which is the process of building a 3D structure by introducing material to a space that previously had none. *Source:* US Army photo by Spc. Adeline Witherspoon, 2nd SBDE PAO. https://www.dvidshub.net/image/5010018/2nd-sustainment-brigade-hosts-armys-first-3d-printer

dynamics, especially established supply chains. These supply chains have already been disrupted by attempts to reshore or move supply chains out of China due to the coronavirus pandemic. In response to the combined technological and geopolitical disruptions, many suppliers across supply-chain tiers will need to identify, certify, and integrate new suppliers and manage new approaches to supply-chain management, none of which will be easy or inexpensive.

In addition, countries across the region will need to balance the need for bilateral and multilateral cooperation in defense technology and capability development and procurement to meet immediate challenges with a longer-term desire across many larger states in the region to establish self-reliance in their domestic defense-industrial bases.

The bilateral Defense Technology and Trade Initiative (DTTI) between the United States and India offers a useful example, though many observers believe this initiative has not yet delivered the hoped-for material results in technology development.

Perhaps a better example of these types of bilateral agreements is the recently reported agreement between Australia and Japan that covers "training and exercises, defence science and technology, and defence industry co-operation and co-ordination on regional issues of shared interest."[71]

This instinct to collaborate to meet immediate challenges is being balanced in all three non-US Quad states (as well as others in the region) by the need to build sustainable

71 Gabriel Dominguez, "Australia, Japan Agree to Deepen Defence Co-operation," *Janes Defence Weekly*, October 19, 2020, https://customer.janes.com/Janes/Display/FG_3772218-JDW.

defense and high-tech industry self-reliance. Australia's "2020 Defence Strategic Update" stresses the need for "strengthened sovereign capabilities to enhance the ADF's self-reliance," especially through leveraging 4IR technologies such as three-dimensional (3D) printing, Internet of Things, and fifth-generation (5G) networks.[72]

India, which is currently among the world's largest defense importers, has been even more vocal in its need to build and reform its defense industry. In August 2020, the government issued a ban on the import of one hundred and one weapons systems and defense items that will be implemented in a phased fashion between now and 2024, allowing India to continue defense technology- and capability-development initiatives, including those covered by the DTTI.[73] The announcement was followed closely by a second announcement from the Defense Research and Development Organization (DRDO) of one hundred and eight technological components and systems that will now be developed domestically—including some unmanned systems—as part of the government's Atmanirbhar Bharat ("Self-Reliant India") initiative.[74]

4. Connectivity, Lethality, and Flexibility: A Revolution in Communication, Navigation, Targeting, and Strike

If the perception, processing, and cognition revolution covers the first three components of the OODA loop, the communication, navigation, targeting, and strike revolution is about enabling the final one: act.

This revolution is centered on innovations in operational capabilities and concepts that will disrupt strategic competitions across several critical military domain areas and help militaries gain advantage in the struggle between power projection and A2/AD efforts.

Technology development in this revolution is designed to enable radically new or enhanced capabilities to

- **communicate** more easily between more numerous and more dispersed systems interacting across multiple domains;
- **navigate** platforms and systems, even in environments in which access to global navigation satellite systems (GNSS) is denied;
- **target** platforms and systems with more precision and flexibility, in order to reduce risk in complex, uncertain, and shifting operational environments; and
- **strike, interdict, or deter** adversary capabilities and assets at short notice, at longer ranges, and in contested environments.

Interest in and development of hypersonic missiles—both hypersonic-glide vehicles and scramjet-based missiles—by China, Russia, the United States, Japan, India, and Australia (which has expressed interest in the weapons) is a clear indicator of the significance of this capability revolution to deterring and responding to an expanding range of defense and security threats in the region. Increasing development of these weapons is also stimulating investment in missile-defense systems and capabilities—from high-end interceptors to hypervelocity projectiles and directed energy, among others.

In addition to the strike versus air- and missile-defense competition, actors across the region are also prioritizing development of novel capabilities associated with this revolution in the undersea domain. Taiwan is moving forward with its own indigenous submarine project while Japan welcomed its new *Taigei* class of submarine into service in October 2020. Australia and other states across the region have ongoing submarine procurement and development programs to meet the growing range of threats in the region.

The nature of weapons systems being developed for the undersea domain goes beyond just crewed submarines.

Indicative Focus Areas of the Communication, Navigation, Targeting, and Strike Revolution in the Indo-Pacific

- Advanced/maneuverable/long-range missiles
- Missile-defense interceptors
- Hyper-velocity projectiles
- Hypersonic missiles
- Drone swarms
- Loitering munitions
- Quantum encryption (specifically, quantum-enabled position, navigation, and timing (PNT))
- Directed-energy weapons
- Railguns
- Electronic attack capabilities
- Advanced anti-submarine warfare capabilities

72 "2020 Defence Strategic Update."

73 "India to Ban Imports of 101 Items of Military Equipment," Associated Press, August 10, 2020, https://thediplomat.com/2020/08/india-to-ban-imports-of-101-items-of-military-equipment/.

74 "DRDO Comes Out with list of 108 Military Systems for Production by Domestic Industry," *Times of India*, August 24, 2020, https://timesofindia.indiatimes.com/india/drdo-comes-out-with-list-of-108-military-systems-for-production-by-domestic-industry/articleshow/77725175.cms.

Australia's "2020 Force Structure Plan" mentions development and deployment of undersea mines as a means of protecting the waterways leading into Australia's sovereign territory, while Japan is developing two prototypes of a remotely operated, self-propelled mine system.[75] These systems are designed to be deployed to high-risk sea areas and loiter there until they are remotely detonated in the proximity of enemy vessels."[76] In October 2020, India's DRDO successfully tested a "game changing" anti-submarine warfare weapon known as the Supersonic Missile Assisted Release of Torpedo (SMART) weapon system, which could allow India's navy to engage adversary submarines beyond torpedo range.[77]

5. Monitoring, Manipulation, and Weaponization: A Revolution in Cyber and Information Operations

The final revolution in the framework addresses how emerging digital technologies are changing the competition in cyber and information operations. The importance of cyber, information, and disinformation operations, both as a means to disrupt societies and polities and to undermine the operational efficacy of adversaries, has been discussed at length above.

However, what has not been addressed as thoroughly is the power of modern technologies, especially AI, to amplify the threat to societies and militaries posed by cyber and information operations.

The Internet Observatory Cyber Policy Center at Stanford University noted in a July 2020 report on China's efforts to shape global narratives and influence political situations in Taiwan and Hong Kong that "today's emergent technologies are enhancing those longstanding capabilities, enabling greater velocity and virality, and offering access to new audiences and ways of spreading information."[78]

AI is at the top of the list of "emergent technologies" influencing developments in both traditional cyber warfare and in the future of information operations. Smart bots, fake AI-generated pictures and profiles, and deepfakes are already being used to influence elections, spread misinformation and disinformation, and harden narratives that could serve as part of gray-zone challenges in the region. Technological advances, as well as refinement of operational concepts, are making the AI-enabled disinformation challenge more difficult to detect and counter. A September 2019 study from researchers at the University of Southern California indicates that bots are getting smarter, and that AI-enabled smart bots make it difficult to distinguish social media interactions with humans from those with bots deployed to manipulate, influence, and outrage. According to the report, "bots better aligned with humans' activity trends, suggesting the hypothesis that some bots have grown more sophisticated."[79]

The Confluence of Social Media Monitoring, Manipulation and Weaponization, and Regional Border Tensions

In July 2020, the Indian Army mandated that personnel delete eighty-nine apps from their mobile phones due to operational security concerns. Banned apps included Facebook, Instagram, and fifty-nine with Chinese links. The Indian Army had previously banned use of WhatsApp for official work in November 2019.

Indian concerns over social media activity are layered. There have been cases in the last several years in which Pakistani agents posing as women have convinced military personnel to divulge classified information. Some military personnel have been court martialled for posting sensitive or classified information—for example, the location of a unit—on social networking websites. In addition, the prevalence of Chinese-developed or Chinese-owned apps also reflects a broader information/cybersecurity concern, especially in light of the recent conflict between China and India.[1]

1 "Army asks soldiers, officers to delete Dailyhunt, Facebook and Instagram; uninstall 89 apps", *The Times of India*, 8 July 2020, https://timesofindia.indiatimes.com/india/army-asks-soldiers-officers-to-delete-dailyhunt-facebook-and-instagram-uninstall-89-apps/articleshow/76858779.cms

75 "2020 Force Structure Plan."

76 Kosuke Takahashi, "Japan Aiming to Develop Prototypes of Self-Propelled Mine System," *Janes*, June 23, 2020, https://www.janes.com/defence-news/news-detail/japan-aiming-to-develop-prototypes-of-self-propelled-mine-system.

77 "India Successfully Tests 'Game Changer' SMART Torpedo System," *Times of India*, October 5, 2020, https://timesofindia.indiatimes.com/india/drdo-successfully-flight-tests-weapon-system-smart/articleshow/78489306.cms.

78 Renee Diresta, et al., "Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives," Stanford Internet Observatory Cyber Policy Center, Hoover Institution, July 2020, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf.

79 Patrick Tucker, "Twitter Bots Are Becoming More Human-Like: Study," *Defense One*, September 6, 2019, https://www.defenseone.com/technology/2019/09/twitter-bots-are-becoming-more-human-study/159697/.

The deepfake challenge is especially acute and concerning. Deepfake technology is growing more sophisticated as well. Even if it remains relatively easy for deepfakes to be detected visually today, this is unlikely to be the case as the technology behind adversarial examples progresses. Perhaps more concerning, deepfake technology is also proliferating widely and being increasingly incorporated in a range of commercial applications—from marketing and advertising to corporate training—which will almost certainly further their distribution.

The combination of technological advancement and general proliferation has created a growing risk for both localized disruption—including from non-state actors—and, more regionally, affecting strategic instability and insecurity as nations employ the technology to create self-serving or destabilizing alternative realities that either reduce the will of targeted populations to resist coercion or, possibly, affect the realities upon which competitor and adversary military and political leaders make decisions.

A January 2020 report from the Bulletin of Atomic Scientists (BAS) stressed the erosion of truth stemming from AI-enabled disinformation campaigns in particular. According to the report, "The recent emergence of so-called 'deepfakes'—audio and video recordings that are essentially undetectable as false—threatens to further undermine the ability of citizens and decision makers to separate truth from fiction."[80]

The good news, if it can be called that, is that the same technologies that are most useful for designing deepfakes and developing particularly agile and effective malicious code are also being used to help detect these malicious threats, reinforcing the interest of defense and broader security communities in these technologies.

But, meeting the challenge will also require additional non-technological innovations, some of which are already taking place in states across the region as recognition of the threat from cyber operations and disinformation campaigns increases. Australia, India, and Singapore, for example, have all established separate defense-focused organizations dedicated to the cyber threat in the last two years.

In addition, countries like Australia and Singapore—through Total Defence—among others, have dedicated resources to expanding the general public's and commercial industry's understanding of the cyber and disinformation threat. Australia's "Cyber Security Strategy 2020" outlines the country's approach "to keeping families, vulnerable Australians, critical infrastructure providers and business secure online" and notes that the strategy is "for all Australians and Australian business." Like Singapore's Total Defence approach, the document stresses that security in the modern strategic and operational environment is "a whole-of-community effort, in which we all have a role to play."[81]

It also sets aside funds—in total, $1.67 billion—to enhance cybersecurity capabilities to "assist industry to protect themselves and raise the community's understanding of how to be secure online."[82]

IV. Key Takeaways and Implications for Strategy and Policy

The changing strategic and operational environment in the Indo-Pacific is helping to drive accelerating innovation efforts among militaries across the region with a particular focus on:

- capitalizing on the digital transformation enabled by the 4IR to develop novel capabilities that can help defense and security communities anticipate and detect subtle and fast-moving challenges that sit at the junction of military and non-military activities and assets;
- building enhanced situational awareness not just to collect information, but also to process it quickly, and multi-mission capability to develop sufficient agility to quickly respond to disparate threats;
- developing the capacity for a range of military responses—including non-kinetic ones such as electronic attack, cyber weapons, and "soft-kill" directed-energy weapons—that offer militaries the flexibility to respond to both traditional and non-traditional threats and challenges in ways that avoid unnecessary escalation or reduce risk to humans—both military personnel and citizens; and
- enhancing the lethality of military forces, largely as a means of deterring actors—particularly China—and being able to bring decisive force to bear in a high-intensity conflict. While such contingencies are generally believed to be unlikely, the intensifying US-China

80 John Mecklin, ed., "It Is 100 Seconds to Midnight: 2020 Doomsday Clock Statement," *Bulletin of the Atomic Scientists*, January 2020, https://thebulletin.org/doomsday-clock/current-time/.

81 "Australian Cyber Security Strategy 2020."

82 Ibid.

> competition has, according to the Australian "2020 Defence Strategic Update," made it more likely than in the recent past.[83]

Achieving these defense technology- and capability-development objectives will require not just identification of and investment in specific technologies or prioritized effects. They will also require innovations in and reconsideration of assumptions about adjacent areas that are critical for militaries to effectively move from a technological breakthrough to an operational military capability, such as organizational structure, defense-industrial engagement and collaboration models, operational concepts, training, and safety and ethics of the development and use of new technologies.

From a policy perspective, the need for both technological and non-technological innovation opens up new and enhanced opportunities for collaboration between the United States and its allies and partners. Recent bilateral and multilateral agreements between the United States and Quad partners, and between individual Quad partners, have included discussion of collaboration on prioritized defense technologies.

This should be encouraged and expanded to ensure a higher degree of interoperability in new technology and capability areas, as well as to amplify the impact of individual technology and capability investments. Further collaboration, especially in establishing common standards and operating procedures for EW and cyber operations, is particularly important, as will be more regular bilateral and multilateral trainings—both live and virtual—that offer opportunities for refinement of operational concepts and common approaches to managing the range of regional security and defense challenges.

83 "2020 Defence Strategic Update."

About the Author

Tate Nurkin is the founder of OTH Intelligence Group and a nonresident senior fellow with *Forward* Defense at the Atlantic Council's Scowcroft Center for Strategy and Security.

Before establishing OTH Intelligence Group in March 2018, Mr. Nurkin spent twelve years at Janes where he served in a variety of roles, including managing Jane's Defense, Risk, and Security Consulting practice. From 2013 until his departure, he served as the founding Executive Director of the Strategic Assessments and Futures Studies (SAFS) Center, which provided thought leadership and customized analysis on global competition in geopolitics, future military capabilities, and the global defense industry.

Substantively, Mr. Nurkin's research and analysis has a particularly strong focus on US-China competition, defense technology, the future of military capabilities, and the global defense industry and its market issues. He also specializes in the design and delivery of alternative futures analysis exercises such as scenario planning, red teaming, and wargaming.

Mr. Nurkin is a frequent author and speaker on these overlapping research priorities. For example, he was the lead author of the US-China Economic and Security Review Commission's report entitled *China's Advanced Weapons Systems*, which was published in May 2018, and has provided testimony to the Commission on two occasions. In March 2019, he was featured on a Center for Strategic and International Studies *China Power* podcast on China's unmanned systems and has subsequently been featured on the *Acquisition Talks* and *Defense and Aerospace Report* podcasts discussing Indo-Pacific military-technology development.

He is the lead author of the Atlantic Council Strategy Paper *A Candle in the Dark: US National Security Strategy for Artificial Intelligence*, which was published in December 2019, as well as the *Emerging Technologies and the Future of US-Japan Defense Collaboration* issue brief published in April 2020.

He previously worked for Joint Management Services, the Strategic Assessment Center of SAIC, and the Modeling, Simulation, Wargaming, and Analysis team of Booz Allen Hamilton. From 2014 – 2018 he served consecutive two-year terms on the World Economic Forum's Nuclear Security Global Agenda Council and its Future Council on International Security, which was established to diagnose and assess the security and defense implications of the Fourth Industrial Revolution.

Mr. Nurkin holds a master of science degree in international affairs from the Sam Nunn School of International Affairs at Georgia Tech and a bachelor of arts in history and political science from Duke University. He lives in Charlotte, NC.

Acknowledgements

This report was made possible with the generous support of Thales Group.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
Matthew C. Bernstein
*Rafic A. Bizri
Linden P. Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Robert S. Gelbard
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Ören
Sally A. Painter
*Ana I. Palacio
*Kostas Pantazopoulos
Carlos Pascual
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

*Executive Committee Members

List as of November 6, 2020

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org