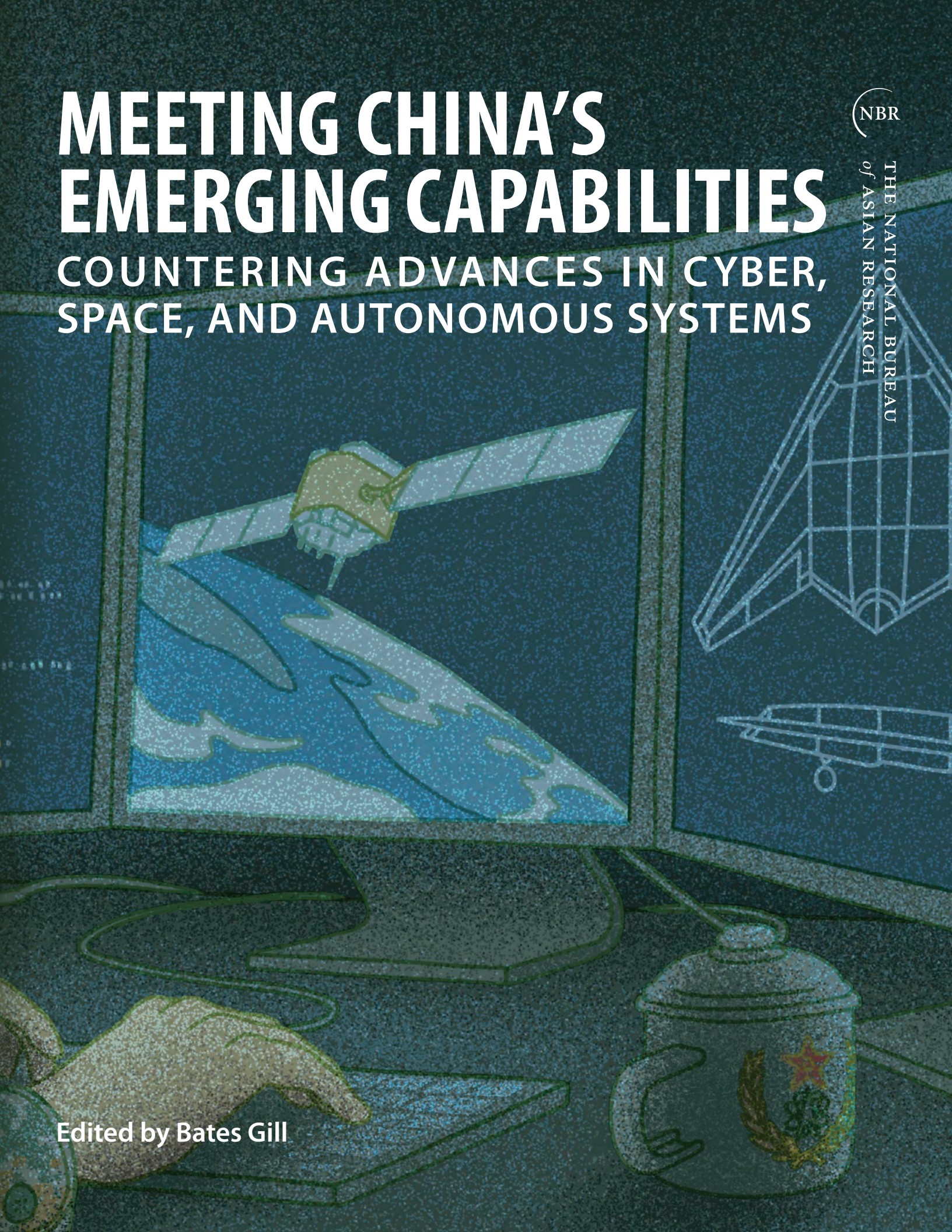
MEETING CHINA'S EMERGING CAPABILITIES

COUNTERING ADVANCES IN CYBER, SPACE, AND AUTONOMOUS SYSTEMS



NBR

THE NATIONAL BUREAU *of* ASIAN RESEARCH

Edited by Bates Gill

THE NATIONAL BUREAU *of* ASIAN RESEARCH
NBR SPECIAL REPORT #103 | DECEMBER 2022

MEETING CHINA'S EMERGING CAPABILITIES

Countering Advances in Cyber, Space, and Autonomous Systems

Edited by
Bates Gill

THE NATIONAL BUREAU *of* ASIAN RESEARCH

The NBR Special Report provides access to current research on special topics conducted by the world's leading experts in Asian affairs. The views expressed in these reports are those of the authors and do not necessarily reflect the views of other NBR research associates or institutions that support NBR.

The National Bureau of Asian Research helps decision-makers better understand Asia and craft concrete, actionable policy. NBR is an independent research institution based in Seattle and Washington, D.C. We bring world-class scholarship to bear on the evolving strategic environment in Asia through original, policy-relevant research, and we invest in our future by training the next generation of Asia specialists.

Our research is conducted by a global network of specialists and tackles critical issues identified by stakeholders in anticipation of future challenges. The findings are a result of independent scholarship and do not reflect institutional perspectives. Our rigorous standards facilitate informed decision-making based on knowledge rather than ideology.

Established in 1989, NBR is a legacy organization of Senator Henry M. Jackson, who foresaw the national need for an institution to study and inform public policy on Asia in both the public and private sectors. Building on Senator Jackson's bipartisan approach, NBR engages policymakers looking for reliable Asia expertise through sustained interaction in high-trust, nonpartisan settings. Our experts and research have shaped congressional legislation and administration policies, brought issues to the top of the U.S. foreign policy agenda, and attracted worldwide media attention. We mobilize expertise on Asia for a more effective foreign policy.

NBR receives support from foundations, corporations, government (including foreign governments of allies and liberal democracies), and public agencies, and philanthropic individuals. NBR reserves the right to publish findings. We do not undertake classified or proprietary research work, and we observe policies to avoid conflicts of interest.

To download issues of the NBR Special Report, please visit the NBR website http://www.nbr.org.

This is the one-hundred-and-third NBR Special Report.

NBR is a tax-exempt, nonprofit corporation under I.R.C. Sec. 501(c)(3), qualified to receive tax-exempt contributions.

Cover design and illustration by Nate Christenson.

For further information about NBR, contact:

The National Bureau of Asian Research
One Union Square
600 University Street, Suite 1012
Seattle, Washington 98101

206-632-7370 Phone
nbr@nbr.org E-mail
http://www.nbr.org

MEETING CHINA'S EMERGING CAPABILITIES

Countering Advances in Cyber, Space, and Autonomous Systems

TABLE OF CONTENTS

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

Introduction: Meeting China's Emerging Capabilities

Bates Gill

BATES GILL is Executive Director of the Asia Society Policy Institute's Center for China Analysis. He is the principal investigator for the National Bureau of Asian Research (NBR) project "Meeting China's Military Challenge: Identifying Collective Responses among U.S. Allies and Security Partners in the Indo-Pacific Region." Dr. Gill previously directed the Stockholm International Peace Research Institute (SIPRI) and held senior research positions with the Brookings Institution and the Center for Strategic and International Studies (CSIS). He can be reached at <bgill@asiasociety.org>.

According to the 2022 U.S. National Security Strategy (NSS), the People's Republic of China (PRC) is the United States' "only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."[1] Among the pathways to this objective, the PRC is "investing in a military that is rapidly modernizing, increasingly capable in the Indo-Pacific, and growing in strength and reach globally—all while seeking to erode U.S. alliances in the region and around the world."[2] With regard to China's military capabilities, the NSS is consistent with the U.S. National Defense Strategy, issued earlier in 2022, which states that the PRC is the United States' "most consequential strategic competitor and the pacing challenge for the Department [of Defense]."[3]

China's ongoing military modernization program—and particularly efforts to develop coercive and deterrent capabilities across multiple domains, such as in advanced aerospace (missilery), cyberspace, outer space, autonomous systems, and weapons of mass destruction—clearly presents a formidable challenge to the United States and its armed forces, especially in the Indo-Pacific. In addition, regional countries, including key U.S. allies and security partners, face similar, often more intense, concerns about China's military capabilities. China poses an increasing threat to the sovereign, territorial, and security interests of many U.S. allies and security partners in the Indo-Pacific, including Australia, India, Japan, the Republic of Korea, the Philippines, the Republic of China (Taiwan), and Vietnam.

However, persistent gaps exist between the shared security concerns of the United States and these partners, on the one hand, and the development and execution of effective collaborative measures these parties can take to counterbalance those concerns, on the other. While in principle officials and researchers understand the need to deepen cooperation with allies and partners in the region to counter China's coercive capabilities, this is difficult in practice at bilateral and especially multilateral levels. In sum, one of the biggest challenges for the United States—but, if surmounted, one of its biggest potential advantages in the region—is developing a greater region-wide understanding and consensus on the security threats China poses and the collective action that can counter them.

To help address this challenge, the National Bureau of Asian Research (NBR), with support from the Defense Threat Reduction Agency Strategic Trends Research Initiative, in 2020 initiated an innovative Track 1.5 research and strategic dialogue project under the title "Meeting China's Military Challenge: Identifying Collective Responses among U.S. Allies and Security Partners in the Indo-Pacific Region." Through commissioned research and dialogue activities, the project aimed to engage experts and government officials from a mix of regional allies and security partners with differing security environments, military capabilities, and relations with China, with a focus on Australia, India, Japan, the Philippines, Taiwan, and Vietnam.

In its first year, the project delivered in-depth research, dialogue, analysis, and recommendations regarding China's most threatening conventional deterrent, coercive, and warfighting capabilities; their effect on U.S. allies and security partners; and options for these governments to partner

[1] White House, *National Security Strategy* (Washington, D.C., October 2022), 23, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[2] Ibid., 24.

[3] "Fact Sheet: 2022 National Defense Strategy," U.S. Department of Defense, March 2022, https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF.

with the United States to effectively counter these challenges. This work was presented in an NBR Special Report released in early 2022.[4]

As in year one, the project's second phase brought together senior experts and government officials from the United States and the same six Indo-Pacific countries—Australia, India, Japan, the Philippines, Taiwan, and Vietnam—through a combination of commissioned research, a virtual workshop held in March 2022, and an in-person, two-day strategic dialogue held in Washington, D.C., in June 2022. In catalyzing research, informed exchanges of information and perspectives, and actionable responses, the project in year two narrowed its focus somewhat and generated critical insights and recommendations on the following questions:

- What specific PRC cyber, space, and autonomous weapons systems present the most credible deterrent, coercive, and warfighting threats to regional security?
- What are some specific scenarios in which the PRC has employed and likely will employ these capabilities against U.S. allies and security partners in the region?
- What specific military policies and operational capabilities have been employed in response by U.S. allies and security partners in the region?
- What specific mechanisms should be considered for Indo-Pacific governments, in partnership with the United States or among themselves, to counter these PRC threats?

This report presents the project findings and recommendations, including the detailed studies by the six country experts commissioned for this iteration of the project. On behalf of NBR, I would like to express my thanks and great appreciation to these experts whose work formed the basis of our strategic dialogue and who are at the very center of the project's success: Francis Domingo of De La Salle University in the Philippines, Peter Jennings of the Australian Strategic Policy Institute, Yuka Koshino of the International Institute for Strategic Studies, Nguyen The Phuong of Ho Chi Minh City University of Economics and Finance, Rajeswari (Raji) Pillai Rajagopalan of the Observer Research Foundation in India, and Yisuo Tzeng of the Institute for National Defense and Security Research in Taiwan.

This introductory essay will provide an overview of the project's findings in year two by focusing on five cross-cutting themes that emerged from the commissioned research and strategic dialogue sessions. It will also put forward a set of nine actionable policy recommendations for the United States that flow from the project's research, analysis, and key findings. Readers seeking more specific country-by-country analysis and recommendations should dive into the excellent country studies—on Australia, India, Japan, the Philippines, Taiwan, and Vietnam—which constitute the remainder of this report.

Wide Variance in Response to PRC Threats

Through the project's commissioned research and dialogue sessions, it became clear there is a wide degree of variance among the experts and government officials involved about the nature and extent of the threat emanating from the PRC's cyber, space, and autonomous systems. Three principal factors appear to explain this divergence: (1) the extent and persistence of PRC threats in these technological realms relative to other threats, (2) the country's ability to respond effectively,

[4] Bates Gill, ed., "Meeting China's Military Challenge: Collective Responses of U.S. Allies and Security Partners," National Bureau of Asian Research, NBR Special Report, no. 96, https://www.nbr.org/publication/meeting-chinas-military-challenge-collective-responses-of-u-s-allies-and-partners.

and (3) the broader strategic, political, and economic environment shaping a country's relations with the PRC. As a result, risks of misunderstandings, misjudgments, and misaligned expectations persist between the United States and key Indo-Pacific partners in response to PRC threats in these realms.

In the case of *Australia*, for example, the country's national security apparatus fully understands that the PRC presents a sophisticated cyberthreat—including through gathering intelligence and engaging in intellectual property (IP) theft, identifying vulnerabilities in critical infrastructure, and conducting covert actions to shape Australian public debate, undermine critics of the PRC, and promote pro-PRC perspectives. Australian strategists also understand that China is developing and deploying space-related and autonomous systems, which present major challenges for the Australian Defence Force (ADF). These systems pose a particular threat to its ability to operate in air and maritime environments, both close to home and as part of coalition operations in such areas as the South and East China Seas.

Australia has taken a number of measures that are in part a response to these developments. These have included substantial new investments in advanced military systems and offensive and defensive cyber capabilities as well as the establishment of the ADF Space Command in January 2022 with a strategy to ensure the armed forces' access to assets in a "congested and contested space environment."[5]

Japan has similar pressing concerns, with three in particular deserving special attention. The first concerns the growing kinetic and nonkinetic anti-satellite (ASAT) and cyberoffensive capabilities of the People's Liberation Army (PLA) and their potential to disrupt and neutralize U.S., Japanese, and allied responses in times of heightened confrontation and conflict. Second, China's rapid development of militarily-relevant space and autonomous technologies can significantly enhance the accuracy and decision-making speed of its offensive threats, especially its ballistic and cruise missiles, potentially undermining the ability to defend Japanese territory and raising questions about U.S. commitments to Japan, including in relation to extended nuclear deterrence. Third, Japan is also the target of persistent cyber-enabled espionage from the PRC, which can weaken the technological advantages of the Japan Self-Defense Forces (JSDF).

In response to these challenges, Japan has taken a number of important steps: it has improved jointness across the JSDF by integrating capabilities across multiple domains, including space and cyber; accelerated investments in capabilities to monitor and respond to Chinese activities in the space and cyber domains; expanded research, development, and deployment of autonomous systems that can deter and disrupt PRC advances, including unmanned underwater vehicles (UUVs), autonomous mine countermeasure systems, and unmanned combat aerial vehicles; and implemented a whole-of-government approach to deter and protect against attacks on government and commercial entities involved in national defense.

However, other countries in the region have more widely divergent responses to PRC threats in these realms. The *Philippines*, for example, is the target of cyber intrusions from China—including attacks to gather intelligence against the Department of Foreign Affairs, the Department of Science and Technology, the Armed Forces of the Philippines (AFP), and Philippine engineering and defense industries. Philippine territorial claims in the South China Sea are also threatened in

[5] Royal Australian Air Force, *Australia's Defence Space Strategy* (Canberra, March 2022), https://www.airforce.gov.au/our-mission/defence-space-strategy.

part by the PRC's vastly superior maritime domain awareness and weapons-targeting capabilities enabled by its space-based intelligence, surveillance, and reconnaissance (ISR).

Yet the Philippine military operates at a far lower level of technological sophistication and struggles to detect and respond to such threats from China, in part because it is focused on other pressing challenges such as domestic insurgencies. The Philippine response to PRC threats has also been hobbled in the past by government policies favoring closer political and economic alignment with Beijing.

Likewise, concerns in *Vietnam* arise from both past and potential future threats from PRC cyber, space, and autonomous systems. Given the malign PRC-based cyber intrusions targeting Vietnam in the past, Vietnamese strategists recognize that China can launch attacks against their country's critical infrastructure and disrupt or distort the flow of information domestically, especially as Vietnam moves to digitize so many elements of its social and economic activities. China's space and autonomous systems provide it with superior targeting and around-the-clock ISR capabilities, which improve its long-range precision-strike weapons, maritime domain awareness, and overall ability to assert and defend claims over territory and resources in the South China Sea that Vietnam also claims.

In spite of these challenges, Vietnam struggles to respond effectively. The chief obstacles include financial, technological, and human resource constraints; a slow-to-reform domestic defense industry; political limitations restricting cooperation in sensitive technology areas with advanced countries such as the United States and others; and continuing reluctance—in part due to party-to-party relations between Beijing and Hanoi—to openly confront China. As a result, for example, Vietnam must rely on foreign commercial sources for satellite imagery and has developed little in the way of concepts and indigenous manufacturing capabilities for sophisticated autonomous systems such as drones for military use.

Like the other countries surveyed in this report, *India* has increasing concerns about China's technological advances in the areas of outer space, cyberspace, and autonomous weapons. Indian analysts see the PLA gaining strategic advantages and "technological asymmetries" that India will find difficult to counter. These concerns result in part from its vulnerability to PRC counterspace capabilities, even as India increases its dependence on space-based assets for social development and military purposes. India is also a victim of China-sourced cyberattacks (including against infrastructure facilities). In addition, Indian strategists are increasingly concerned about China's ability to prosecute more fast-paced and lethal military campaigns enabled by artificial intelligence (AI) and autonomous systems.

In recent years, India has begun establishing institutional, technological, and military responses to these threats. This includes measures to mitigate cyber intrusions, protect critical infrastructure, and develop and deploy ASAT weapons, autonomous systems such as drones and UUVs, and cyberwarfare concepts and capabilities. However, these steps face limitations. For example, regarding ASATs, one Indian test thus far is probably not enough demonstrated capability to deter China. These steps are also limited by budgetary constraints, an over-reliance on India's own defense industrial base for the development of advanced systems, and the need to pour resources into a manpower-intensive defense of India's disputed borders with China and Pakistan.

In comparison to the other five countries considered in this project, *Taiwan* faces the most persistent and dangerous threats from China's space, cyber, and autonomous systems. These

threats would be especially acute in the event of a concerted attack on Taiwan. China would likely employ advanced persistent threat and distributed denial-of-service attacks against critical infrastructure and cyber and counterspace attacks against Taiwan's communications satellites and their ground stations. In addition, Taiwan would face precision missile attacks enabled by PRC satellite-based ISR, navigation and guidance systems, and deployments of aerial, sea surface/subsurface, and ground-based autonomous systems for surveillance and strike missions. However, with the exception of developing greater resilience in its cyberdefenses, Taiwan has been slow to develop capabilities that can counter PRC threats in realms such as space and autonomous systems.

Urgent Sense of "Falling Behind"

The commissioned research and dialogue discussions of this project reveal an increasing sense of urgency across the region that countries are falling behind in response to China's technological advances in autonomous-, space-, and cyber-related military systems. Three principal factors can explain this situation: (1) a lack of investment in capabilities that could deter or counter PRC developments in these areas, (2) a lack of sufficient human and military-technical capacity in critical technology areas, and (3) hesitancy to openly counter or confront China's military advances. Overall, participants in the project agreed that the rate of military technological change by China seems to be outpacing the necessary policy responses by regional governments.

In the case of *Australia*, for example, significant resources have been committed to deliver major weapons platforms—"megaprojects" such as submarines and large surface ships—in the mid to late 2030s. However, China's rapid advances in certain military technologies are forcing Australia to overhaul its force structure priorities in order to fill capability gaps in the near term. The most pressing priorities are those systems that can hold PRC assets at risk farther from Australian shores. These include such procurements as Tomahawk cruise missiles, long-range anti-ship missiles, and precision-strike guided missiles for ADF land forces. Importantly, Australia aims to develop an indigenous guided-weapons manufacturing capability, expand its over-the-horizon radar capability, and deepen cooperation with the United States in the development of hypersonic weapons. These steps will accompany significantly boosted investments in defensive and offensive cyber capabilities. But the planned procurements face a number of challenges and, at best, will take years to put in place.

At present, except for deployed forces, Australia has no current or planned capability for expanded ballistic missile defenses. It also scrapped plans to procure and operate a low-cost, multirole, long-endurance drone such as the U.S. MQ-9B SkyGuardian. Moreover, Australian strategists and political leaders continue to express concerns in the near term (the next five to ten years) about the survivability of forward-deployed maritime platforms and the ability of the national cyber infrastructure to withstand incursions from China. Without mentioning China by name, Australia's *2020 Defence Strategic Update* warns that "new capabilities, including longer-range missiles, ballistic missiles, and offensive cyber and space capabilities have reduced strategic warning times."[6] In addition, China's development and deployment of large numbers of relatively inexpensive and expendable autonomous systems could overwhelm ADF platforms, which are high-performing but few in number.

[6] Department of Defence (Australia), *2020 Defence Strategic Update* (Canberra, July 2020), https://www.defence.gov.au/about/publications/2020-defence-strategic-update.

This project's research and dialogue revealed that for *Japan* the PRC's growing capabilities in autonomous, space, and cyber systems may hasten the pace of Chinese military modernization in ways that might undermine U.S. deterrence in defense of Japan. Concerns include Japanese vulnerabilities in the face of concerted PRC cyberattacks and cyber extrusions aimed at critical infrastructure and defense-related government agencies, research institutes, and companies, which could weaken the JSDF's technological advantages. Participants also expressed concern that China may rush its development of autonomous military capabilities and use them in contingencies in the East China Sea and around Taiwan, even though they may be unsafe or unreliable and could unnecessarily escalate a military engagement with Japan.

Japanese leaders recognize these vulnerabilities, and support for expanding the country's ability to close these gaps is on the rise—perhaps best illustrated by the government's decision to increase defense spending to 2% of GDP in the next five years and invest more heavily in capabilities necessary for deterrence and warfighting in new domains such as autonomous, space, and cyber systems. However, serious challenges will restrain a speedy realization of these efforts. First, Japan still struggles with leveraging academic R&D for military end-use. Even though the 2021 *Defense of Japan* white paper placed an unprecedented degree of urgency on the need to strengthen the country's defense-industrial base to achieve "technological superiority" in emergent military-technical realms, and the Ministry of Defense has established programs to foster basic academic research for defense purposes, academic institutions often remain reluctant to engage in this kind of work. Second, Japan's weak information security system, including the lack of a unified vetting process for persons engaged in sensitive national security activities, undermines close collaboration within Japan across the government, industry, and academia and between these institutions and foreign counterparts.

Because they are close allies of the United States and relatively wealthy, Australia and Japan have comparatively greater access to systems and technologies that can counter PRC threats. This is not the case for others in the region. The *Philippines*, for example, lags far behind the PRC across the full range of military capabilities and especially in terms of space, cyber, and autonomous systems. It is still in the earliest stages of enhancing its ability to detect and respond to PRC threats enabled by these technologies. For example, Philippine national security agencies have only in recent years begun to develop cyber capabilities for defense purposes and aim to build the capacity to observe and assess the space-related activities of others.

Philippine cyber capabilities are in their formative stages, and the country's space program is modest at best. Moreover, the AFP will primarily concentrate on the development of more traditional conventional capabilities—such as naval platforms, anti-ship weapons, and counterinsurgency warfare—before it considers more effective countermeasures to the PLA's autonomous, cyber, and space weapons systems. Indeed, there is little to no evidence that the AFP is considering the use of or defense against autonomous weapons systems as part of its officially declared military modernization program. In fact, autonomous weapons systems are hardly mentioned in recent national security strategy documents.

Vietnam likewise faces a growing gap in its capabilities vis-à-vis China, particularly in more advanced military-technical areas enabled by space, cyber, and autonomous systems. Especially concerning for Vietnamese strategists is the lack of sufficient maritime defense awareness to monitor and effectively respond to activities in the South China Sea, which may threaten Vietnam's national interests. Many gray-zone activities on China's part—which seek to assert and secure

PRC territorial claims in disputed waters without escalating to outright conflict—are enabled by its capabilities in the cyber, space, and autonomous realms and have already advanced the PRC's de facto control over large areas of the South China Sea. Vietnam has been slow to respond to these developments due to political, budgetary, and human resource constraints. Meanwhile, the PLA continues to strengthen its capabilities in such advanced technologies.

In many ways, India and Taiwan face some of the most direct threats from China's cyber, space, and autonomous weapons systems. Yet they too have been relatively slow to react, portending a widening gap between their capabilities and those of China.

As recognized by strategists in *India*, continuing development of these capabilities by the PLA may undermine Indian deterrence, thereby emboldening more assertive military action by China, especially in contested areas along the Sino-Indian border. India confronts the growing reality that increasing technological asymmetry favors China, including in the cyber, space, and autonomous realms, and that these developments have given China advantages that can tilt the military balance conclusively in its direction. It is true that the Indian government and its defense research establishment aim to prepare the Indian armed forces for next-generation warfare—particularly in reaction to PRC investments in emerging technologies—with the long-range goal to shift from a manpower-intensive to a technology-enabled force. But a significant gap remains between those objectives and the necessary procurements and deployments that India needs to keep up with its giant neighbor to the north.

Leaders and strategists from *Taiwan* are well aware of the growing capabilities gap they face vis-à-vis the PLA. In response, Taiwan has embraced such principles as "fortress Taiwan," the "porcupine strategy," and an overall defense concept, all names for approaches to deter and thwart a PRC invasion through the effective use of asymmetric warfare. This strategy aims to consolidate and build redundancy and resilience into Taiwan's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) infrastructure; bolster passive and active defensive countermeasures against aerial and maritime threats; and develop more lethal and longer-range precision counterstrike capabilities, including offensive cyber missions.

However, concerns persist in the United States and in Taiwan about Taipei's commitment to these plans. For example, Taiwan has limited space-based or counterspace capabilities of its own and is highly reliant on foreign commercial space assets for much of its communications and intelligence. It is not developing any ASAT capabilities at this time. Notably, Taipei has increased its focus on the development of indigenous autonomous systems to counterbalance China's advances in this technology area. However, in spite of that increased focus, Taiwan's efforts remain far behind those of China and may be "too little too late." In the words of one prominent strategist from Taiwan taking part in the project, "time is not on Taiwan's side as China has been accelerating its military modernization in every domain, with salient progress in cyber, space, and autonomous weapons."

Drawing Lessons from the Ongoing War in Ukraine

In many respects, it remains too early to confidently predict the precise impact that the Russia-Ukraine war will have on regional security elsewhere. Clearly, that conflict has elevated the importance of space, cyber, and autonomous assets, and Indo-Pacific leaders and strategists are following these developments very closely in three areas in particular: (1) what the war reveals

about the changing nature of modern warfare, (2) how it may affect the PRC's calculations for asserting its interests in the region through military coercion or the use of force, and (3) what the war in Ukraine may portend for conflict across the Taiwan Strait.

Across the research and dialogue sessions of this project, there was widespread consensus that the war in Ukraine has further underscored the importance of new modes of warfare enabled by cyber, space, and autonomous systems. Such technologies have proved their value in supporting both surveillance and strike roles and acting as relatively inexpensive force multipliers. Much attention has been focused on how Ukraine has managed to use such technologies to its advantage against a more powerful Russian military. For example, it gained significant advantage in the field through the integration of relatively simple military and commercial drones with access to advanced targeting and intelligence inputs.

Of course, lessons from the war in Ukraine are not only useful to "underdogs." Larger powers, such as China as well as Russia itself, are also drawing lessons from the conflict. China will undoubtedly further hone the use of its cyber, space, and autonomous systems. Such systems can be effective as gray-zone weapons, acting to strengthen coercion and deterrence without necessarily prompting an escalation to open conflict, and in many instances can overwhelm less capable forces in China's periphery that do not have effective countermeasures in place.

Across the region, such developments are sparking new concerns about China's military intentions and capabilities in the Indo-Pacific. In Japan, for example, Russia's use of cyberattacks in the early phases of its invasions of Ukraine in 2014 and 2022, including attempts to disable Ukrainian nuclear power plants, has raised concerns about possible PRC cyberattacks against critical infrastructure, including as means to deter Japan's involvement in a Taiwan contingency. More broadly, the Russian invasion of Ukraine and the role of technological domains such as cyber, unmanned aerial vehicles (UAVs), and space-related assets in the conflict give greater momentum to arguments in support of increasing defense spending in Japan, including in these and other areas of future warfighting.

For Taiwan, the war in Ukraine has apparently catalyzed a far more focused discussion about how to achieve its porcupine strategy. At the same time, most Taiwan defense experts agree that direct and overly simplistic comparisons of the Ukraine and Taiwan cases should be avoided. Ongoing discussions, debates, wargaming, and tabletop exercises continue in Taiwan to carefully discern the current state of the PRC threat and the lessons that should inform its strategy going forward.

Some early takeaways have gained traction in these debates. First and foremost, Taiwan must build resilience and redundancy across both physical and virtual domains, and building such resilience and redundancy takes time. In many respects, Taiwan is today more accustomed to hostile cyberoperations and is better prepared for them than Ukraine was at the outset of Russia's 2022 invasion. However, unlike Ukraine, Taiwan is not connected to neighboring states via land-based fiber networks and must rely on undersea cables and satellites. This potential vulnerability leads Taiwan to try to learn from Ukrainian success in establishing multiple channels of communications redundancy, including, if possible, collaboration with like-minded governments for access to satellite communications and intelligence.

Second, the Ukrainian use of precision-guided weapons to sink Russian naval vessels, shoot down Russian aircraft, and destroy Russian armored columns helps bolster elements of Taiwan's overall "porcupine" approach. In particular, these developments in Ukraine suggest that Taiwan is

on the right track by increasing the procurement, storage, and protected deployment of seaborne anti-ship cruise missiles, land-based mobile anti-ship and anti-air missile platforms, and the corresponding mobile radar surveillance, microwave communications, and decoy platforms.

But the war in Ukraine also underscores Taiwan's immense need for large, readily resupplied stockpiles of light, mobile, precise weapons enabled by sophisticated intelligence and targeting assets, which should be prioritized over large, expensive, and sophisticated weapon platforms. While UAVs are in demand for Taiwan's armed forces, Taiwan has a limited supply of U.S. MQ-9 and domestically produced drones. Perhaps more importantly, it remains highly uncertain whether, in the event of a conflict, Taiwan will have sufficient access to the battlefield intelligence, including from foreign sources, required to make such autonomous systems fully effective.

In addition, Taiwan has drawn important lessons in other areas. One notable example is the need to develop redundant and resilient offensive and defensive capabilities in relation to cyber, electronic, space, and autonomous systems warfare, as well as improving cognitive operations and the training necessary to effectively fight in conflict conditions defined by these technological realms. The conflict in Ukraine suggests that a greater demonstrated capability in these areas—possibly including through cooperative initiatives with the United States—could have a deterrent effect on the PRC.

Implications for Deterrence and Weapons of Mass Destruction

The PRC's emergent advances in space, cyber, and autonomous weapons systems have larger and potentially serious implications for the country's approach to deterrence and weapons of mass destruction (WMDs). As China continues to modernize across the spectrum of militarily relevant technologies, strategists in the United States and across the region are in the early stages of fully understanding how these developments affect Beijing's evolving calculus of deterrence and its possible uses of WMDs. In some ways that lack of understanding and increased ambiguity alone may serve as a deterrent advantage for Beijing.

The integration of these technologies into China's conceptual and operational calculus for WMDs makes a complicated situation all the more complicated. Importantly, the project's deliberations identified an increasing regional concern over China's ability to deter the United States and, moreover, to test the United States' resolve, resilience, and responses beneath the conflict threshold. In particular, the PLA's successful integration of these technologies into its strategic and conventional operations may lower the threshold for WMD use by China—either by accident or by design—and can sow doubt in U.S. resolve, in U.S. extended nuclear deterrent commitments to allies in the region, and in the confidence other partners have in Washington's defense commitments in the region more broadly.

Several key points deserve particular attention. First, China's expanding constellation of land- and space-based assets has led to improvements in its nuclear weapons arsenal—including improved targeting, improved early-warning capabilities, and improved air defenses. These developments in turn open the door to adjustments in China's long-standing "no first use" pledge, including the possibility of a "launch on warning" posture. Relatedly, project participants pointed out that, with China's increased reliance on space- and cyber-related assets in support of its nuclear weapons, an attack on those assets could prompt an escalatory response from China if it believed those strikes were meant to compromise or disarm its nuclear deterrent.

Second, China is likely seeking to develop and integrate AI, autonomous capabilities, and cyber resiliency into its strategic weapons systems and supporting infrastructure. This could lead to greater confidence among PRC political leaders and military commanders regarding threat discernment, targeting, and launch decisions and the protection of their own command and control channels. This in turn raises the possibility of overconfidence and miscalculation in weapons use, at both the conventional and unconventional levels.

Third, if and as China gains confidence in the ability to deter the United States at the nuclear level, it may prompt greater escalatory measures on Beijing's part in the conventional realm. If it can keep such a clash beneath the nuclear threshold, Beijing may believe that it can fight and win a conventional conflict by inflicting unacceptable damage on U.S. forces, especially in areas close to the PRC's periphery where it wields many advantages in terms of proximity, concentration of firepower, and resupply logistics. Under these circumstances, China may be more likely to confront and combat the United States in increasingly threatening ways. This could include attacks on the long-serving multi-mission satellites and sophisticated cyber-enabled communications networks on which the U.S. military relies—strikes that Beijing may believe are "conventional" rather than "strategic" in nature.

Fourth, these technological and operational developments for China prompt concerns among U.S. allies about the scope and reliability of extended nuclear deterrence. Of particular relevance for the project's focus on cyber, space, and autonomous systems, China's test of a nuclear-capable hypersonic glide vehicle in 2021 raises new concerns about its anti-access/area-denial capabilities and prompt global strike (including nuclear strike) and the challenges they may pose to U.S. deterrence commitments.

Expanding Partnerships with the United States and Others

The commissioned research and strategic dialogue discussions generally underscored a continuing strong demand for the United States to be more deeply engaged in the Indo-Pacific region, including in helping regional governments respond more effectively to the threats posed by the PRC's development of cyber, space, and autonomous weapons systems. These discussions also revealed a greater degree of cooperation among regional governments and others, in addition to the United States, to counter PRC threats. Project findings further underscore a pressing need to deepen U.S.-Taiwan collaboration, especially in areas of advanced technologies where Taiwan lags considerably behind.

However, the extent and nature of those partnerships vary widely across the different countries assessed in the project. Overall, collaboration in these technological areas among regional partners remains in the early stages. It ranges from deepening military-technical and intelligence cooperation between the United States and close partners, such as Australia and Japan, to more modest measures, such as technological cooperation among civilian scientists and nonlethal defense equipment sales with countries such as Vietnam.

Australia will further deepen its long-standing military-technical partnership with the United States and with others. The Australia–United Kingdom–United States (AUKUS) partnership, announced in September 2021, is the most promising vehicle for strengthening Australia's ability to counter PRC threats, including those in the cyber, space, and autonomous realms. Although much attention will be focused on Australia's ability to develop and deploy nuclear-propelled

submarines, the agreement also very importantly covers a wide range of other militarily relevant technologies and platforms such as undersea defense and long-range strike capabilities, quantum technologies, AI, electronic warfare, and hypersonic weapons.

In addition, Australia's establishment of the Defence Space Command in 2022 and its release of a new defense space policy will help frame and deepen already-robust U.S.-Australia space-related cooperation. It is highly likely that such cooperation will continue to focus on countering PLA capabilities. U.S.-Australia cooperation in cyberspace remains close and involves both defensive and offensive elements. Interestingly, the Quadrilateral Security Dialogue (the Quad) among Australia, India, Japan, and the United States established a Senior Cyber Group to share information on cybersecurity, cyber resilience, and critical infrastructure protection in the Indo-Pacific. But given Australia's relatively slow start in developing autonomous capabilities, it must cooperate far more closely with the United States and others, including to develop strategies to counter the PLA's growing capabilities in this technological realm.

Driven in large part by China's growing military capabilities, *Japan* has been increasingly open to developing stronger bilateral and multilateral defense cooperation with the United States and others, including in relation to cyber, space, and autonomous systems. This is accomplished through strategic alignment mechanisms such as the U.S.-Japan Security Consultative Committee (also known as 2+2) and through more specific official dialogue mechanisms on space and cyber cooperation. Importantly, the 2019 2+2 joint statement affirmed "that international law applies in cyberspace and that a cyber-attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty."[7]

At the 2022 2+2 ministerial meetings, both sides noted their "concerns about the large-scale development and deployment of nuclear weapons, ballistic and cruise missiles, and advanced weapons systems such as hypersonics"; flagged the "increasing malign activities in the cyber, space, and other domains"; and underscored the critical need for the alliance to strengthen "cross-domain capabilities, particularly integrating the land, maritime, air, missile defense, space, cyber, electromagnetic spectrum, and other domains."[8] It will be critical for the Alliance Coordination Mechanism, established in 2015, to step up to facilitate this kind of deeper coordination between U.S. and Japanese armed forces and defense establishments. Of particular note, Japan has also deepened defense-related cooperation with Australia and the UK in recent years through conducting joint exercises and by opening up the prospect for greater defense-industrial cooperation.

For the *Philippines*, the most practical and promising strategy to counter emerging technology threats from China is to strengthen its political-military alliance with the United States. That relationship sustained considerable damage in recent years, including during the administration of Rodrigo Duterte as Philippine president from 2016 to 2022.

That said, the Philippines still receives approximately $125 million each year in various military assistance programs from the United States. To date, however, this assistance has not given a strong focus to emerging technological areas such as cyber, space, and autonomous weapons systems. With a newly elected government in Manila in 2022, a fresh opportunity exists to open a range

[7] "Joint Statement of the Security Consultative Committee," Ministry of Foreign Affairs (Japan), April 19, 2019, https://www.mofa.go.jp/files/000470738.pdf.

[8] "Joint Statement of the U.S.-Japan Security Consultative Committee ('2+2')," U.S. Department of State, January 6, 2022, https://www.state.gov/joint-statement-of-the-u-s-japan-security-consultative-committee-22.

of discussions to bolster the U.S.-Philippines military-technical relationship, including in these technology areas.

In response to shared threat perceptions about China, *India* and the United States have deepened their partnership in emerging technology areas, including space and cybersecurity. It is possible, according to some indications, that the United States assisted India by providing intelligence during the clashes in Galwan and Ladakh. The United States has also increased its military-technical cooperation with India, including through arms sales and defense science and technology exchanges. As the Quad gains momentum, it also fosters cooperative exchanges between India and the United States (as well as the other two Quad partners, Australia and Japan) on a range of technology issues, including space and cyber.

In addition to its partnerships with the United States and other Quad members, India is stepping up partnerships with other countries on these critical and emerging technologies. On cybersecurity, for example, the Indian Computer Emergency Response Team, an agency under the Ministry of Electronics and Information Technology, has concluded agreements with Japan, Malaysia, and Singapore to focus on trends in cybersecurity incidents, updated information on the latest threats, and best practices to augment cybersecurity.

Options for *Taiwan* to collaborate with the United States and others in the defense field are constrained by the unique and unofficial nature of Taiwan's diplomatic relations and concerns over how the PRC will react to those countries' ties with Taiwan. Nonetheless, the United States and Taiwan have deepened their partnership in recent years in both the political and defense spheres.

Arms sales form a high-profile aspect of those ties, but other official and quasi-official consultations in relation to Taiwan's defense also continue. However, it is unclear in the unclassified realm to what degree this cooperation involves exchanges in the cyber, space, and autonomous domains. This project highlights China's growing capabilities in these areas, the threats they pose to Taiwan, and the need for Taiwan to significantly bolster its offensive and defensive capabilities in the face of these challenges. This provides an opportunity for the United States to strengthen cooperation with Taiwan in the cyber, space, and autonomous realms, including demonstrable, public strengthening of the island's deterrence posture.

Of the six countries considered in this project, *Vietnam* has the lowest degree of partnership and trust with the United States, especially regarding security and defense. While steadily improving since the countries established diplomatic relations in 1995, bilateral relations are still constrained by an undercurrent of strategic mistrust and lingering animosity, making it difficult to collaborate on sensitive issues, including military-technical cooperation and intelligence sharing. Moreover, Vietnam remains highly reliant on arms supplies from Russia, though it has opened its doors to defense-related exports from countries such as India, Israel, the Netherlands, and South Korea, as well as the United States.

Encouragingly, Washington and Hanoi are engaged in several defense-related collaborations that over time could build trust and facilitate more robust military-technical cooperation. These include U.S. assistance to remove unexploded ordnance, support through the Department of Defense Cooperative Threat Reduction Program, the State Department Maritime Security Initiative, the provision of Hamilton-class coast guard cutters, and exports of other defense items such as fire control, lasers, imaging and guidance equipment, military electronics, and UAVs. Much of this support aims to improve Vietnam's maritime domain awareness. Owing to Russia's invasion of Ukraine and the subsequent sanctions on Moscow, as well as to concerns about an

over-reliance on Russian weaponry, debate continues among Vietnamese policymakers about possibly diminishing the country's dependence on Russian arms exports.

Policy Responses

Based on the overarching themes outlined in the previous sections, and drawing from the detailed, country-specific findings in the following essays, this section presents nine actionable policy recommendations for the U.S. government and particularly for the U.S. Department of Defense. These recommendations are intended to help improve the ability of the United States, in collaboration with its Indo-Pacific allies and partners, to counter growing PRC coercive, deterrent, and warfighting threats enabled by cyber, space, and autonomous systems.

Recommendation 1. The Office of the Secretary of Defense, U.S. Indo-Pacific Command, and other relevant agencies should further deepen consultations with key regional partners in relation to cyber, space, and autonomous technologies and the threats they pose from China, with a focus on and appreciation for the particular circumstances these partners face. These discussions should be accompanied by greater intelligence sharing and public use of intelligence, as appropriate, to build regional consensus in both bilateral and multilateral settings in response to PRC threats in these technological areas. Official bilateral and multilateral statements in summit, "2+2," and other senior leadership meetings should include specific mention of PRC provocations in the cyber, space, and autonomous spheres.

Recommendation 2. The Department of Defense, its relevant agencies, and key interagency partners should give even greater priority to investments in hardware, software, training, and joint operational coordination in partnership with regional allies—especially Australia and Japan—in the defensive and offensive application of cyber, space, and autonomous technologies, with PRC capabilities particularly in mind. Certain partners such as the Philippines and Taiwan should receive accelerated assistance in the development, procurement, and deployment of space-related and autonomous assets to support much-needed reconnaissance and precision-strike capabilities. This effort must focus on building resilience, redundancy, and resupply into the procurement and deployment of these and other military systems by the United States and its partners in the Indo-Pacific, especially for Australia, Japan, the Philippines, and Taiwan. This urgent need can be met through expansion of joint R&D and manufacturing facilities, hardened infrastructure, and significantly increased pre-positioning of materiel in these and other partner countries in the region.

Recommendation 3. U.S. civilian and defense intelligence agencies should prioritize assessing China's interpretation of the Russia-Ukraine conflict. In particular, they should study how U.S., allied, and Ukrainian responses have affected Beijing's thinking about achieving its preferred outcomes through the threat and use of military force in the region, including toward Taiwan, but not exclusively so. Such information and analysis should be shared, as appropriate, with allies and partners to help build collective preparedness and shared purpose in the region.

Recommendation 4. U.S. civilian and defense intelligence agencies should actively consider and judiciously deploy "weaponized" intelligence to publicly expose PRC activities of concern and strengthen deterrence capabilities of the United States and its partners in the face of PRC threats. This effort should selectively reveal ongoing U.S. defense collaboration programs with key partners in the region; demonstrate U.S. and partner capabilities, including in the areas of cyber,

space, and autonomous systems; and shed light on threatening plans and activities of the PLA prior to their execution.

Recommendation 5. Given the relevance of developments in Ukraine for Taiwan, the Office of the Secretary of Defense, U.S. Indo-Pacific Command, the American Institute in Taiwan, and other relevant defense and interagency partners should engage even more actively with Taiwan counterparts to develop coordinated communications and operational awareness platforms, expand the parameters for U.S.-Taiwan cybersecurity cooperation, enhance Taiwan's reconnaissance and precision-targeting capabilities, and build resilience, redundancy, and resupply capacity, including in the cyber and autonomous domains.

Recommendation 6. U.S. civilian and defense intelligence agencies, in coordination with interagency analytical and policy communities, should invest greater resources in understanding and responding to the PRC's calculus of deterrence and escalation control both above and below the WMD threshold. They should also invest resources in better dissuading and disrupting China's growing confidence and risk-taking in its deterrence posture.

Recommendation 7. The United States should increase defense budgetary resources to bolster its deterrent and extended deterrence commitments, in both word and deed, including through diversification and strengthening of strategic conventional and nuclear weapons, delivery platforms, and supporting infrastructure. Greater capacities should also be developed, both unilaterally and in consultation with key allies, for holding critical PRC cyber and space assets at risk and signaling the will and capacity to do so.

Recommendation 8. The Defense Threat Reduction Agency should increase its engagement and support of allies and partners in the Indo-Pacific region to develop capacities to monitor, assess, and counter WMD threats from the PRC, including China's WMD-enabling technologies in the cyber, space, and autonomous realms. Special attention should be given to assist less-resourced allies and partners such as the Philippines, Taiwan, and Vietnam.

Recommendation 9. Despite the emergent and sometimes sensitive nature of cooperation in the cyber, space, and autonomous realms, the Office of the Secretary of Defense, the Joint Staff J5 (Strategy, Plans, and Policy), and other relevant defense and interagency partners should give urgent priority to reversing gaps between PLA cyber, space, and autonomous capabilities and the ability of Indo-Pacific allies and partners to effectively counter them. The greatest priority should be focused on defensive and offensive cyber capabilities; improved reconnaissance, surveillance, and precision targeting; and the production, effective operational deployment, and resupply of autonomous weapons systems. It is especially urgent to support Taiwan in the acquisition and demonstrated use of such asymmetric capabilities as part of its overall defense operations concept.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

The Implications of China's Military Modernization for Australia and Regional Security

Peter Jennings

PETER JENNINGS is the CEO of Peter Jennings Strategy Consultants and a Senior Fellow at the Australian Strategic Policy Institute (ASPI). He previously served as the executive director of ASPI. He can be reached at <peterjennings@aspi.org.au>.

EXECUTIVE SUMMARY

This essay examines the cyber, space, and autonomous systems developed and deployed by the People's Republic of China (PRC), outlines the steps Australia has already taken to respond to these challenges, and considers options for how Australia can partner with the U.S.

MAIN ARGUMENT

The rise of an assertive PRC seeking within the decade to build large-scale military capabilities to challenge the U.S.-led international security order in the Indo-Pacific presents immediate challenges to Australia's security. This is leading to a rapid Australian reassessment of its own military capabilities within the context of a close alliance with the U.S. The emphasis is increasingly on acquiring or developing military capabilities that will strengthen the Australian Defence Force (ADF).

POLICY IMPLICATIONS

- The Australian reassessment of its military capability priorities also creates a period of immense opportunity to rethink technological, strategic, and operational cooperation with the U.S. The AUKUS agreement between Australia, the United Kingdom, and the U.S. potentially enables a trilateral pooling of defense, science, technology, and industrial capabilities that could produce new military capabilities in areas such as hypersonics, quantum computing, and cyber technology.
- Australia is looking to develop a domestic missile production capability and to acquire a series of longer-range weapons across the ADF, which would also be of use to the U.S. for its military stockholding and production needs in the Indo-Pacific.
- While Australia continues to plan for the long-term replacement of submarines and surface ships, a new emphasis on autonomous systems, cyber capability, cooperation on space security, and smart long-range weapons holds open the prospect of building a better-armed ADF within the current decade.
- These are promising developments that will strengthen Australia's military capabilities and contribute to a closer alliance relationship with the U.S., but it is early in the process. The biggest risk to successful cooperation is that the two countries' considerable bureaucratic and institutional processes slow down or get in the way of shared innovation.

Australia increasingly views the rise of an assertive People's Republic of China (PRC) as the central challenge to stability in the Indo-Pacific. After years of benefiting from China's economic growth, successive Australian federal governments in Canberra have become much more pessimistic and focused on Beijing's overt challenge to the international rule of law. This does not necessarily translate into a direct PRC military threat to the Australian landmass. Yet Australians historically think of their security as being tied to a stable international order, to which the country contributes as a responsible middle power, as an ally of the United States, and with a small but technologically advanced defense force.

Since 2019, there has been a sharp deterioration in Australia-PRC relations over Beijing's management of Covid-19 and opposition to Canberra's policy to exclude PRC companies from the rollout of Australia's 5G network. Australian defense planners are sharply aware of the PRC's interest in establishing a larger military presence in the Pacific Islands, in intrusive PRC naval activities around the country, and in PRC cyber, espionage, and covert political interference activities. As such, the PRC is seen as presenting a significant strategic threat to Australian interests, a threat that is underpinned by its substantial and growing military capabilities.

This essay surveys the cyber, space, and autonomous systems developed and deployed by the PRC and the principal threats they pose to Australia's defense capabilities. It then outlines the steps Australia has taken to counter these challenges and puts forward recommendations for how Australia, in partnership with the United States, can better counter threats from the PRC's development of its cyber, space, and autonomous weapons system capabilities in the Indo-Pacific.

Emerging PRC Cyber, Space, and Autonomous Weapons System Capabilities

Cyber-Related Systems

Australia is under daily barrage from PRC-sourced cyber systems designed to achieve malign effects, including intelligence gathering and intellectual property (IP) theft; attempts to identify vulnerabilities in critical infrastructure and, according to some reports, the prepositioning of malware able to disrupt critical infrastructure operations; and covert actions designed to shape the public debate, undermine critics of the PRC, and promote pro-PRC perspectives.

A particular focus of PRC interest is the Australian Defence Force (ADF), the Defence Department, and the wider national security and intelligence apparatus. Government national security information technology (IT) systems, especially classified systems, have higher levels of cyber protection and a workforce trained in personal and information security. Nevertheless, the national security system understands that the PRC is a sophisticated and persistent cyberthreat. Recent examples include the following:

- The Ministry of State Security's exploitation of vulnerabilities in Microsoft Exchange software was identified by the Australian, U.S., and other governments in July 2021. The New Zealand government identified the hostile cyber actor as Advanced Persistent Threat 40.[1] This group

[1] Andrew Little, "New Zealand Condemns Malicious Cyber Activity by Chinese State-Sponsored Actors," Beehive (New Zealand), Media Release, July 19, 2021, https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors.

has been reported on by Mandiant as "a cyber counterpart to China's efforts to modernize its naval capabilities."[2]

- In February 2019, the federal government identified a sophisticated cyberoperation to hack into the computer systems of Australia's major political parties. Senior intelligence sources briefed media outlets that the PRC was the source of the attack, reportedly saying, "It's been a long time since we've been faced with an actor with this level of sophistication. This trade craft is good. This actor is good."[3] It subsequently emerged that the intrusion was much wider than the major political parties and included security agencies.

While at this stage there are no specific attacks on Australian critical infrastructure clearly attributed to the PRC by government sources, this is an area of increasing national security focus. The chair of the Parliamentary Joint Intelligence and Security Committee, Senator James Paterson, told the *Australian* newspaper in October 2021: "Economic coercion has not worked as well against us as they may have hoped but cyber-attacks emanating from China against government entities and critical infrastructure providers [are] absolutely relentless and there's much more we need to do to harden ourselves against these incursions."[4]

PRC cyber-enabled threats to critical infrastructure present perhaps the most direct warfighting threat to Australia because of the absolute dependence of the ADF on national economic infrastructure to supply, power, sustain, and maintain operations for any extended period. For example, in September 2021, Australian national holdings of crude oil and refinery feedstocks were estimated by the government to be sufficient for 31 days of normal usage.[5] The ADF would draw on those resources in any crisis and does not maintain separate supplies. Cyberattacks on critical infrastructure for holding and distributing crude oil and refinery feedstocks would have significant short- and long-term impacts on the ADF's capacity to conduct operations.

Cyberespionage and influencing attempts may have less direct impacts on military capabilities but are nevertheless significant. IP theft from defense industry suppliers, for example, could compromise the classified capabilities of ADF weapons systems. The penchant of PRC state and party actors for IP theft of big data could yield militarily useful information about the location and activities of ADF personnel, readiness levels, and operating routines.

Space-Related Systems

Of the plethora of relevant PRC space-related systems, the People's Liberation Army (PLA) Navy's efforts to develop a robust space system–enabled over-the-horizon targeting capability to optimize its use of anti-ship cruise missiles (ASCMs) fired from both submarines and surface vessels is of immediate concern to the ADF's ability to conduct operations. The Luyang III–class guided-missile destroyers and Renhai-class guided-missile cruisers are fitted with, respectively, 64-cell and 112-cell vertical launching systems capable of launching cruise missiles. They are being equipped with the new YJ-18A cruise missile, which has a publicly assessed range of 290 nautical miles. The PLA Navy Aviation Service has, according to the U.S. Department of Defense, "begun

---

[2] "Advanced Persistent Threats (APTs)," Mandiant, https://www.mandiant.com/resources/apt-groups.

[3] Andrew Tillett, "Chinese Spies Suspected in Cyber Attack on Major Parties," *Australian Financial Review*, February 18, 2019, https://www.afr.com/politics/cyber-attack-on-major-parties-computer-systems-scott-morrison-reveals-20190218-h1bdzm.

[4] Cameron Stewart, "China Biggest Threat to Way of Life, Says Senator James Paterson," *Australian*, October 8, 2021, https://www.theaustralian.com.au/nation/china-biggest-threat-to-way-of-life-says-senator-james-paterson/news-story/fb31930251b60d60e302a70d9ae068e7.

[5] Department of Industry, Science, Energy and Resources (Australia), "Australian Petroleum Statistics," September 2021, 74, https://www.energy.gov.au/sites/default/files/Australian%20Petroleum%20Statistics%20-%20Issue%20302%20September%202021.pdf.

operating the H-6J, a maritime strike version of the H-6K with six weapons pylons for ASCMs. This aircraft carries six supersonic long-range YJ-12 ASCMs and can attack warships out to the Second Island Chain."[6]

This is of particular concern to Australia for operations in the South China Sea. The government's *2016 Defence White Paper*, which remains the basis for force structure planning, identifies "maritime Southeast Asia" as a key strategic priority, in particular: "In Southeast Asia, Defence will strengthen its engagement, including helping to build the effectiveness of regional operations to address shared security challenges, and the ADF will have increased capabilities to make contributions to any such operations."[7] The extent to which Australia can deliver on that aspiration rests heavily on the survivability of its forward-deployed maritime platforms operating in coalition or as part of a joint ADF mission. Therefore, the PLA's capacity to use space assets to monitor, target, and track enemy forces is a critical strategic factor.

A second area of direct Australian concern relates to PRC long-range ballistic missiles. Australia's *2020 Defence Strategic Update*, released in July 2020, states that "new capabilities, including longer-range missiles, ballistic missiles and offensive cyber and space capabilities, have reduced strategic warning times."[8] In this context, the U.S. Department of Defense's 2021 report to Congress on Chinese military and security developments finds that the PLA controls "around half" of the PRC's 200-strong reconnaissance and remote-sensing satellite fleet and is working hard to improve its capabilities to track and target adversaries' forces.[9] Other than for deployed forces, Australia has no current capability or plans to develop ballistic missile defense capabilities.

The PRC's growing but publicly unacknowledged anti-satellite capabilities for conducting low-earth-orbit missions and, potentially, for targeting geosynchronous satellites present a third area of obvious concern, negatively affecting Australian and allied military operations in the Indo-Pacific. The *Strategic Update 2020* states that "assured access to space is critical to ADF warfighting effectiveness, situational awareness and the delivery of real-time communications and information." Plans for increased Defence Department investments in space-related systems include deploying "a network of satellites to provide an independent and sovereign communications network and an enhanced space control program."[10] Notwithstanding the reference to an independent and sovereign communications network, the reality is that Australia collaborates closely with the United States on space situational awareness, including sensors and tracking systems.

The Defence Space Strategy released in February 2022 acknowledges that "Defence has limited sovereign space capabilities and therefore leverages agreements with the United States, other international partners and commercial entities for many space capabilities." It further identifies five immediate priorities:

1. Enhance Defence's space capability to assure Joint Force access in a congested and contested space environment.
2. Deliver military effects integrated across Whole of Government and with allies and partners in support of Australia's national security.

---

[6] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2021* (Washington, D.C., November 2021), https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

[7] Department of Defence (Australia), *2016 Defence White Paper* (Canberra, February 2016), 17, https://www.defence.gov.au/about/publications/2016-defence-white-paper.

[8] Department of Defence (Australia), *2020 Defence Strategic Update* (Canberra, July 2020), https://www.defence.gov.au/about/publications/2020-defence-strategic-update.

[9] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2021*, 67.

[10] Department of Defence (Australia), *2020 Defence Strategic Update*.

3. Increase the national understanding of the criticality of space.
4. Advance Australia's sovereign space capability to support the development of a sustainable national space enterprise.
5. Evolve the Defence Space Enterprise to ensure a coherent, efficient and effective use of the space domain.[11]

An ADF Australian space command was established in January 2022 under the command of Air Vice-Marshal Catherine Roberts. These developments show promising new momentum in the Defence Department's approach to space, which has not had the priority it deserved in past years. Although Australia has cooperated closely with the United States on space policy (discussed further below), there is an opportunity emerging to enhance that cooperation, including on how to address the operational challenges presented by China's space-based and space-enabled capabilities. In launching a space command, former defence minister Peter Dutton, who now leads the opposition party, acknowledged "that some countries are developing capabilities to threaten or degrade space networks, to target satellites, and to destroy space systems." Dutton said that space "is a domain which must be used to deter aggression, rather than become a new realm for conflict."[12] Determining precisely how Australia and the United States can work together to achieve that deterrent effect or otherwise complicate the PRC's approaches remains a promising area for cooperation.

Autonomous Weapons Systems

The PRC is developing a wide range of autonomous systems in the land, sea, and air domains with the intention of achieving global leadership in those areas. Those systems could present significant challenges for the ADF, but given Australia's strategic geography, air and sea autonomous systems present the most credible deterrent, coercive, and warfighting threats. Key PRC systems include high-altitude and long-endurance unmanned aerial vehicles (UAVs), such as the WZ-7 Soaring Dragon; high-performance unmanned combat aerial vehicles, such as the Hongdu GJ-11 Sharp Sword; and a high-speed WZ-8 UAV.[13] China is also pursuing maritime autonomous systems, and an unmanned underwater vehicle controlled by artificial intelligence (AI), known as the HSU-001, is in development.[14]

Those systems could present risks to ADF and coalition operations in the East and South China Seas, potentially complicating access through critical chokepoints such as the Malacca Strait and the Indonesian archipelago. A proliferation of large numbers of relatively low-cost autonomous systems might threaten to overwhelm the self-defense capabilities of ADF platforms, of which Australia maintains small numbers of capable systems. As a consequence, ADF and allied

---

11 Department of Defence (Australia), *Australia's Defence Space Strategy* (Canberra, February 2022), https://www.airforce.gov.au/our-mission/defence-space-strategy.

12 Peter Dutton (address to the 2022 Royal Australian Air Force Air and Space Power Conference, Canberra, March 22, 2022), https://www.minister.defence.gov.au/minister/peter-dutton/speeches/address-2022-royal-australian-air-force-air-and-space-power.

13 Andreas Rupprecht and Gabriel Dominguez, "Chinese Air Force Equips 16th Air Division with WZ-7 HALE UAVs," Janes, November 11, 2021, https://www.janes.com/defence-news/news-detail/chinese-air-force-equips-16th-air-division-with-wz-7-hale-uavs; Joseph Trevithick, "China Showcases Stealthier Sharp Sword Unmanned Combat Air Vehicle Configuration," Drive, October 1, 2019, https://www.thedrive.com/the-war-zone/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration; and Tyler Rogoway, "China Appears Set to Unveil Very High-Speed Drone during Big Military Parade in Beijing," Drive, September 15, 2019, https://www.thedrive.com/the-war-zone/29857/china-appears-set-to-unveil-a-very-high-speed-drone-during-big-beijing-military-parade.

14 H.I. Sutton, "Chinese HSU-001 LDUUV Large Displacement Unmanned Underwater Vehicle," Covert Shores, October 2, 2019, http://www.hisutton.com/Chinese_LDUUV.html.

platforms may be constrained to operate at greater distances from hostile targets, complicating targeting.

PRC sea mines may also present serious challenges to ADF and coalition maritime operations inside the first island chain. As in all areas of military capability, the PRC is actively interested in sea mines, minelaying, and minesweeping. Recent PLA exercises around Taiwan have included minelaying by H-6J aircraft.[15] Offensive PRC use of sea mines could threaten Australia's naval bases and civil port infrastructure, along with access through chokepoints and into the South China Sea.

Australian Responses

The rapid pace of the PRC's military capability development, along with its increasingly aggressive posture in the Indo-Pacific, is forcing a dramatic recalibration of Australian defense policy thinking. With the *2016 Defence White Paper*, Australia embarked on an ambitious force structure renewal plan, but the bulk of the investment effort was locked into a series of "megaprojects"—submarines, frigates, and a renewal of the army vehicle fleet—that will not produce fieldable capabilities until (in the case of the navy projects) well into the 2030s. While those projects remain in place, the current focus of government attention is on strengthening the ADF's capabilities in the short term.

Key new force structure objectives include the following:

- Tomahawk cruise missiles, to be fielded on the navy's Hobart-class destroyers
- joint air-to-surface standoff missiles to equip the air force's F/A-18F Super Hornets and, in the future, F-35A Lightning IIs
- long-range anti-ship missiles for the Super Hornet
- collaboration with the United States to develop hypersonic missiles
- precision-strike missiles for land forces with a range of over 400 kilometers
- a projected AU$1 billion commitment for a "sovereign guided weapons manufacturing enterprise"[16]

Missile acquisitions are possible in the short term through the U.S. Foreign Military Sales program and are ongoing. It will take some years to ready the ADF for cruise missiles. Plans to manufacture missiles in Australia aim to see production begin around the mid-2020s. The missile manufacturing plan is most likely to become a joint arrangement with one or more manufacturers that already have missiles in service with the ADF. An essential outcome should be to provide a source of redundancy, expansion, and supply for the United States and potentially other allies in the region. Canberra announced in April 2022 that "Raytheon and Lockheed Martin have been chosen to deliver the Sovereign Guided Weapons and Explosive Ordnance Enterprise (GWEO), to initially enhance self-reliance and supply chain resilience, but with a future goal of developing

[15] "China Laying Mines, Dropping Bombs in Taiwan Strait to Deter U.S., Allies," *Business Standard*, December 10, 2021, https://www.business-standard.com/article/international/china-laying-mines-dropping-bombs-in-taiwan-strait-to-deter-us-allies-121121000295_1.html.

[16] "Media Statement: Australia to Pursue Nuclear-Powered Submarines through New Trilateral Enhanced Security Partnership," Prime Minister of Australia, https://www.pm.gov.au/media/australia-pursue-nuclear-powered-submarines-through-new-trilateral-enhanced-security.

a guided weapons manufacturing capability in Australia."[17] This project will support U.S. missile requirements in the Indo-Pacific while expanding the ADF's missile stockholdings and capabilities.

After decades of neglect and allowing already limited mine-hunting capabilities to run down, the Department of Defence has announced a plan to "enhance mine warfare capabilities for the Australian Defence Force to secure Australia's maritime approaches, using modern, smart sea mines."[18] Sea mines would complicate the capacity of an adversary to approach Australian military bases and commercial ports. Used to defend the approaches to Australia's north and to the country's vital ports, sea mines could hamper PLA movements through chokepoints in the Indonesian archipelago. Used as offensive weapons, sea mines might complicate the operations of PLA vessels in the South China Sea. The advantages of sea mines are that they are relatively easy to quickly acquire from a variety of sources and can be deployed from multiple different platforms.

Significantly, the *2020 Defence Strategic Update* announced the expansion of Australia's over-the-horizon radar network to include a new capability "to provide wide area surveillance of Australia's eastern approaches." The existing network looks north and west.[19] This is particularly relevant in the context of the PRC looking to establish closer security cooperation with a number of Pacific Island countries and following the successful conclusion of a security agreement between the PRC and the Solomon Islands (against Australia's wishes) in June 2022.[20]

The difficult reality is that many of Australia's key defense capability development plans are intended to deliver major platforms from around the middle of the 2030s. This particularly affects Australia's acquisitions of submarines and major surface combatants. To some extent, Australian planners have been surprised by the pace of the PRC's military capability development, its activities in Southeast Asia and the Pacific, and the increased aggression of Beijing's behavior and rhetoric. This is forcing a rapid reassessment of Australian force structure priorities, with an intent to deliver significant deterrence-enhancing capabilities to the ADF as soon as possible. The arrival of the Australian Labor Party government on May 21, 2022, has triggered further reviews of force structure plans. Both sides of Australian politics seem to be accepting of the proposition that defense spending will need to significantly grow beyond the current level of 2% of GDP.

Operationally focused defense cooperation on cyber matters is less visible at an unclassified level but is an area of increased priority, reflecting a shared U.S. and Australian view that the cyber domain will be an integral part of future warfighting. Australia's most recent defense policy statement, the *2020 Defense Strategic Update*, points to the need to develop "capabilities to hold adversary forces and infrastructure at risk further from Australia, such as longer-range strike weapons, cyber capabilities and area denial systems."[21] A substantial boost to cyber investments was made in the March 2022 budget. Project REDSPICE—standing for resilience, effects, defense, space, intelligence, cyber, and enablers—claims to be "the most significant single investment" in the history of the Australian Signals Directorate (ASD). The project plans to invest an additional AU$9.9 billion in funding over the coming decade in a range of areas, including tripling the size of

---

17 "Raytheon and Lockheed Martin to Deliver GWEO," *Australian Defence Magazine*, April 5, 2022, https://www.australiandefence.com.au/defence/joint/raytheon-and-lockheed-martin-to-deliver-gweo.

18 Department of Defence (Australia), "Maritime Mining," 2021, https://www.defence.gov.au/project/maritime-mining.

19 Department of Defence (Australia), *2020 Defence Strategic Update*.

20 Peter McCutcheon, "China-Solomon Islands Security Deal Could Lead to a 'Difficult' Situation for Australian Troops in Honiara," ABC News (Australia), June 8, 2022, https://www.abc.net.au/news/2022-06-08/solomon-islands-china-security-australian-and-chinese-troops/101134982.

21 Department of Defence (Australia), *2020 Defence Strategic Update*.

the ASD's offensive cyber capability. Notwithstanding the reference to defensive cyberoperations, Australian government agencies explicitly state that the ASD actively engages in offensive cyberoperations. The ASD's annual report for 2020–21 says: "Offensive cyber operations involve a broad range of offshore activities designed to deter, disrupt, degrade and deny adversaries, in support of Government national security priorities…ASD's offensive cyber operations provide effective and timely support for military operations in accordance with Australian Defence Force priorities and requirements."[22]

In sum, while the Australian Defence Organisation finds itself under enormous pressure to reshape planning at the same time that strategic developments are demanding immediate responses, this is also a period of immense opportunity to rethink technological, strategic, and operational cooperation with the United States.

Partnering with the United States

Autonomous Weapons Systems

The ADF's record on integrating autonomous platforms into the force structure is not strong. The ADF, for example, remains one of the few advanced defense forces to not be operating an armed UAV. The March 2022 budget rather puzzlingly decided to abandon a decade-long plan to acquire the MQ-9B SkyGuardian long-endurance drone. The drone would have been configured to provide armed support to ground forces, but it can be optimized to perform a range of intelligence, surveillance, and reconnaissance roles. In April 2022, the Japan Coast Guard announced that it would begin operating the SeaGuardian version of this drone in October, with the possibility that the Japan Maritime Self-Defense Force will follow suit. At the beginning of May 2022, the U.S. Marine Corps also confirmed that it would acquire eighteen of these drones, known in its system as the MQ-9A, and has plans to double that number.

Australia could have chosen to be part of a coalition of countries operating a low-cost drone that is available now, with the capacity to remain airborne for twenty hours and the ability to perform a variety of missions, from conducting maritime surveillance to supporting ground troops with missiles. A drone of the MQ-9B type has potentially useful applications in a high-threat environment where Australia will be reluctant to deploy its small number of piloted aircraft. The Australian Defence Organisation indicated that the decision to cancel the SkyGuardian acquisition was taken by the government in part to free funds for investment into the REDSPICE cyber project. If nothing else, this is a lesson in the difficulties facing a small defense force where opportunity costs and trade-offs are always difficult and resource constraints are constantly present.[23] Before the May election, the then opposition Labor Party said it would review the SkyGuardian cancellation. In government, the new Labor defense minister Richard Marles has declined to address the future of the program other than to say that he would be "applying a critical eye to the integrated investment plan."[24]

---

22 Australian Signals Directorate (ASD), *Annual Report 2020–21* (Canberra, September 2021), 29, https://www.asd.gov.au/annual-reports.

23 Peter Jennings, "We Must Learn Defence Lessons from Ukraine," *Australian*, May 14, 2022, https://www.theaustralian.com.au/inquirer/we-must-learn-defence-lessons-from-ukraine/news-story/aead0f9952fdf96b1be32e15ec6ef0eb.

24 Daniel Hurst, "Labor to Rethink Coalition's 'Bewildering' Decision to Scrap Armed Drones If It Wins Election," *Guardian*, April 20, 2022, https://www.theguardian.com/australia-news/2022/apr/20/labor-to-rethink-coalitions-bewildering-decision-to-scrap-armed-drones-if-it-wins-election; and "Interview with Greg Jennett, ABC News," Department of Defence (Australia), Transcript, June 7, 2022, https://www.minister.defence.gov.au/minister/rmarles/transcripts/interview-greg-jennett-abc-news.

One further development worth noting is the announcement made by former defense minister Dutton during Australia's May 2022 election campaign that Australia plans to fast-track the acquisition of three extra-large autonomous undersea vehicles. For a planned cost of US$100 million, the boats are to be built in Australia over three years in a co-development project between the Australian Defence Organisation and U.S. company Anduril.[25] The boats are said to be capable of long endurance and multi-mission roles. While much remains to be decided, not least whether the newly elected center-left Labor government will continue with the project, it is pleasing to see the Defence Organisation take some tentative steps toward developing autonomous systems. Clearly, these and other recent force structure decisions are driven by a sense of the emerging threat from the PRC and the risk that PLA capabilities present to ADF operations involving limited numbers of highly expensive and crewed platforms.

Given Australia's slow start in developing autonomous capabilities, there is significant room for closer collaboration with the United States, particularly taking into consideration strategies to counter PLA capabilities in this area. For example, Australia should join its partners within AUKUS (the United Kingdom and the United States) or the Quad framework (India, Japan, and the United States) to establish a working group focused on countering PRC autonomous systems. The aim should be to pool data on PRC capabilities and to turn around tactical responses in rapid timeframes. One lesson emerging from the Russian invasion of Ukraine is that Ukraine has derived significant battlefield advantages from combining simple military and commercial off-the-shelf aerial drones with a sophisticated and flexible targeting infrastructure. The PRC will undoubtedly be absorbing that lesson, but it is one that Australia and the United States should also consider, in terms of both how to apply these tactics and how to defend against them.

In the Australia-U.S. context, collaboration on how to counter PRC autonomous systems will have immediate application in terms of interoperability because the two countries' forces work together seamlessly. There is clearly more work needed to achieve a similar degree of interoperability with Japan in trilateral cooperation, although significant progress is being made. In the case of India, while defense interaction is growing, true interoperability is a long way off.

AUKUS is the most promising vehicle for trilateral cooperation because of the closeness of Australia, the UK, and the United States in intelligence and defense cooperation. Although a key initial focus of AUKUS is on shaping the most effective pathway for Australia to develop nuclear-propelled submarines, it is important to note that the agreement covers a wide range of technology opportunities, including autonomous systems and cybersecurity. AUKUS is significant because it reflects a commitment on the part of U.S., UK, and Australian leadership to change past forms of cooperation. The agreement's focus is squarely on the Indo-Pacific, and the PRC, without being named, is the obvious source of concern. The inaugural joint leaders statement set out an ambitious agenda for change:

> We will promote deeper information and technology sharing. We will foster deeper integration of security and defense-related science, technology, industrial bases, and supply chains. And in particular, we will significantly deepen cooperation on a range of security and defense capabilities.[26]

---

[25] Andrew McLaughlin, "Anduril & ADF to Partner on Autonomous Undersea Vehicle Development," *Australian Defence Business Review*, May 5, 2022, https://adbr.com.au/anduril-adf-to-partner-on-autonomous-undersea-vehicle-development.

[26] "Joint Leaders Statement on AUKUS," White House, September 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus.

One should not underestimate the challenges, particularly in changing defense capability development and acquisition processes in the three countries, but thus far, momentum appears to have delivered satisfactory progress. In April 2022, the AUKUS leaders reviewed progress in implementation and stated the following about autonomous systems: "Through the AUKUS Undersea Robotics Autonomous Systems (AURAS) project, our nations are collaborating on autonomous underwater vehicles, which will be a significant force multiplier for our maritime forces. Initial trials and experimentation of this capability are planned for 2023."[27]

Australia's Labor government has pledged bipartisan support for AUKUS, although there are elements of the Labor Party's membership that retain concerns about nuclear propulsion. Notwithstanding the system-changing complexities that AUKUS presents, it is currently the most promising sign of energized defense and security cooperation between the three countries and will help give momentum to closer collaboration on a range of technologies, driven by a shared concern about the PRC's strategic intentions.

In terms of new opportunities for cooperation, Australia should develop a shared plan for an autonomous counter-mine warfare capability, perhaps building on the Anglo-French joint maritime mine countermeasures program that handed a demonstrator capability to the Royal Navy in November 2021.[28] The United States and Australia should undertake a fast-paced development program designed to deliver a relatively simple smart mine with multiple delivery capabilities. The two countries should also develop a "bolt-on" anti–autonomous vehicle capability for maritime platforms under swarm attack.

Cyber Systems

Australian cooperation with the United States on cybersecurity is particularly deep and based on a signals intelligence relationship going back to World War II. In 1956, the ASD (then the Defence Signals Bureau) joined the United Kingdom–United States Agreement, which forms the basis for the Five Eyes intelligence-sharing partnership between Australia, the UK, the United States, Canada, and New Zealand. Signals intelligence cooperation between the Five Eyes partners is remarkably integrated, involving intelligence sharing, personnel exchanges, joint operational activity, and shared capability development. This level of close cooperation has extended into the cyber domain.

In September 2011, following the annual Australia-U.S. ministerial meeting in San Francisco, the two countries issued a statement, for the first time identifying cyberattacks as falling under the provisions of the ANZUS Treaty:

> We recognize that cyberspace plays a growing role in ensuring national security. Mindful of our longstanding defense relationship and the 1951 Security Treaty between Australia, New Zealand, and the United States of America (ANZUS Treaty), our Governments share the view that, in the event of a cyberattack that threatens the territorial integrity, political independence

[27] White House, "Implementation of the Australia–United Kingdom–United States Partnership (AUKUS)," Fact Sheet, April 5, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus.

[28] "UK: First Delivery of MMCM Remotely-Operated Boat to Royal Navy," Navy Recognition, December 9, 2021, https://www.navyrecognition.com/index.php/naval-news/naval-news-archive/2021/december/11096-uk-first-delivery-of-mmcm-remotely-operated-boat-to-royal-navy.html.

> or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.[29]

At a senior level since 2019, the annual Australia-U.S. Cyber Dialogue has provided strategic direction to achieve what the ASD describes as "full-spectrum and integrated cyber superiority through the combined development of cyber capabilities." At the 2022 dialogue, senior leaders from the ADF, the ASD, and U.S. Cyber Command discussed "how to ensure collective advantage in cyberspace through integration across the areas of defensive cyber operations, capability development, training and exercises."[30]

The bulk of defense-related cyber cooperative activity is classified, but a substantial amount of cooperation is taking place, much of it focused on China and Russia. One public example of coordinated action involving the United States, Australia, the UK, and European Union partners was a decision in July 2021 to name China's Ministry of State Security as engaging with "criminal contract hackers to conduct unsanctioned cyber operations globally, including for their own personal profit."[31] This related to an exploitation of vulnerabilities in Microsoft Exchange software affecting thousands of computers and networks worldwide, including in Australia. The Australian government issued a statement indicating that it was "seriously concerned about reports from our international partners that China's Ministry of State Security is engaging contract hackers who have carried out cyber-enabled intellectual property theft for personal gain and to provide commercial advantage to the Chinese Government."[32]

At the unclassified level, it is clear that Australian cooperation with the United States on cyber is close, involves both defensive and offensive components, has a strong focus on the PRC, and has an increasing willingness to "name and shame" Beijing's malicious cyber activities. Another interesting feature is the broadening of this cooperation to involve multiple like-minded international partners. For example, in March 2022 a "Quad Senior Cyber Group met in Sydney for two productive days of discussions on opportunities to extend our cybersecurity cooperation and uplift cyber resilience and critical infrastructure protection in our region."[33]

Following the coordinated announcements in 2021 about the PRC's use of commercial groups to attack thousands of organizations via vulnerabilities in the Microsoft Exchange software, the United States and Australia should establish protocols for more regular "naming and shaming" of PRC malign cyber actors. This does seem to have some impact on PRC behavior. In addition, the two countries should establish an Australia-U.S. government–private sector partnership on critical infrastructure security. This would lift problems with the vulnerability of such infrastructure to the cabinet level in both countries and the boardrooms of major owners. Australia and the United States should also develop joint and combined deployable military units focused on applying strategic and tactical offensive cyber capabilities for Indo-Pacific operations.

---

29 "Cooperation on Cyber: A New Dimension of the U.S. Alliance," Parliament of Australia, Media Release, September 15, 2011, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F1095105%22;src1=sm1.

30 "AUS-US Cyber Dialogue 2022," ASD, Media Release, https://www.asd.gov.au/publications/aus-us-cyber-dialogue-2022.

31 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, Press Release, July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china.

32 Jane Norman, "Australia Joins International Community in Blaming China for Large Scale Microsoft Hack," ABC News (Australia), July 19, 2021, https://www.abc.net.au/news/2021-07-19/australia-us-uk-blame-china-for-microsoft-hack/100305934.

33 "Statement by National Security Council Spokesperson Emily Horne on Quad Senior Cyber Group Meeting," White House, March 25, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/statement-by-national-security-council-spokesperson-emily-horne-on-quad-senior-cyber-group-meeting.

In terms of cooperation with the United States, the ASD claims that Project REDSPICE will enable "greater integration through expanded global footprint, co-investment in Five-Eyes initiatives [and] collaboration on AI and cyber technologies."[34] The project looks to set the template for Australia and U.S. cooperation on cybersecurity. The following lists of major activities are the ASD's public summary of the project.[35]

Scaled cyber effects of Project REDSPICE include the following:

- triples the offensive cyber effects capability to support the ADF
- supports the integration of the ADF information warfare and cyber workforce
- deepens technology cooperation with allies and partners
- contributes to integrated deterrence

New intelligence capabilities of Project REDSPICE include the following:

- enhances intelligence capabilities that help prevent strategic surprise
- informs decisions of consequence and minimizes miscalculation
- increases understanding of adversaries' capabilities, intent, and decision-making
- doubles the analytic workforce

Enhanced national cyber defense of Project REDSPICE includes the following:

- improves resilience of critical infrastructure against sophisticated cyberattacks
- increases the visibility of threats to Australia's most critical systems
- improves machine-time cyber threat intelligence sharing across government and industry
- doubles persistent cyber-hunt activities and nationwide cyber-incident response

Increased resilience and redundancy of Project REDSPICE include the following:

- increases resilience of classified communications capabilities
- creates redundancy in critical capabilities through national and international dispersal
- employs 40% of the ASD workforce outside Canberra
- increases Australia's overseas footprint fourfold

Improved foundational technologies of Project REDSPICE include the following:

- delivers new cloud-based cyber and intelligence systems and applications
- scales up AI and machine-learning capabilities
- delivers AI-supported offensive and defensive cyber capabilities

All of this will take place in the context of close alliance cooperation with the United States and shows a major increase in capability directed at understanding and countering the PRC.

Space-Related Systems

The establishment of a defense space command and the release of a defense space policy set the context for Australia-U.S. cooperation on space matters. Much classified engagement is

[34] ASD, "REDSPICE: A Blueprint for Growing ASD's Capabilities," https://www.asd.gov.au/about/redspice.

[35] Ibid.

underway, while publicly the Australian emphasis has been on pressing the PRC to be a responsible international actor in space. Although that diplomatic approach will continue, it is highly likely that Australia and the United States will be able to focus classified cooperation more sharply on countering PLA capabilities.

To support that objective, the United States and Australia should establish a joint defense and intelligence community working group focused on how to most effectively disrupt PLA air and maritime targeting and command, control, communications, and intelligence (C3I) capabilities. Such discussions could also address options and approaches to prepare for disruption operations focused on PLA C3I. In addition, the two governments should determine operational protocols for coalition operations in circumstances in which their C3I capabilities may be disrupted.

Conclusion

Defense cooperation between the United States and Australia is extremely close and has emphasized a high level of interoperability, which has been regularly tested in combat operations. One indication of the unparalleled level of trust between the national security communities of both countries is President Joe Biden's remarkable decision to allow Australia access to U.S. nuclear propulsion technology for submarines. The arrival of AUKUS suggests that Australia and the United States can deepen security cooperation even further by pooling science, technological, and defense industry capabilities and identifying collaborative projects aimed at quickly fielding new military capabilities. Although significant differences in scale exist between the military, technology, and industry sectors of both countries, Australia has high-quality IP and creativity to bring to the table.

A new factor driving this deepening cooperation is the PRC, which is aggressively working to supplant the United States as the dominant strategic power in the Indo-Pacific. Australia and the United States have the same apprehensions about Beijing's intentions, as indeed do most of the world's consequential democracies. The growth of PRC military power and Beijing's increasingly belligerent behavior in the East and South China Seas, in cyberspace, and elsewhere have added a sense of urgency to the agenda for Australia-U.S. defense cooperation. The need, in short, is for fieldable military capabilities to strengthen deterrence within years rather than decades.

The options set out in this essay point to specific possibilities for defense cooperation in capability development as well as force posture and operational planning—a list that is by no means exhaustive. The biggest risk to successful cooperation is that the two countries' considerable bureaucratic and institutional processes slow down or get in the way of shared innovation. In whatever way Australia and the United States approach this problem, the current need is to move quickly and apply lateral thinking to what they can achieve together.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

China's Military Modernization in Autonomous, Cyber, and Space Weapons: Implications for Taiwan

Yisuo Tzeng

YISUO TZENG is an Assistant Research Fellow of the Cyber Warfare and Information Security Division at the Institute for National Defense and Security Research in Taiwan. He can be reached at <yisuo.tzeng@indsr.org.tw>.

EXECUTIVE SUMMARY

This essay finds that given China's acceleration of its military modernization in cyber, autonomous, and space weapons in recent years, coupled with the lessons drawn from Russia's war in Ukraine, Taiwan will need to speed up the pace in procurement, staffing, and training and brace for asymmetric joint operations.

MAIN ARGUMENT

China's autonomous-, cyber-, and space-related systems will play an important role in both gray-zone coercion and the warfighting threats confronting Taiwan and other like-minded regional partners across the entire spectrum of threat contingencies, from incursions to invasion. To that end, China is most likely to resort to hybrid threats, such as cyber-electromagnetic operations to achieve cognitive effects or space-electromagnetic operations to disrupt and block Taiwan's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Kinetic missile attacks by the People's Liberation Army (PLA)—with target acquisition powered by Gaofen-series reconnaissance satellites and navigation guided and timed by the BeiDou satellite system—would worsen the situation on the ground and lead to widespread fear and confusion. In the meantime, the PLA could selectively leave certain communication backbone networks functional to allow information, disinformation, and influence operations to convey images of climbing death tolls, horrifying damage, and, most importantly, panic. These kinds of operations would likely be waged and implemented throughout the whole process of a PLA invasion. The software-defined radio apparatuses installed in unmanned aerial vehicles (UAVs) capable of communication relay allow for the creation of self-organizing networks and thereby possess counter-electromagnetic capabilities in defense of Taiwan's air-defense systems.

POLICY IMPLICATIONS

- Training in information operations, particularly the psychological operations training sessions and workshops that the U.S. military provides in the U.S. and Taiwan, would greatly assist Taiwan's special operations forces, reserve forces, and political warfare officers.
- The U.S. should collaborate more closely with Taiwan's advanced information technology industry in the development, manufacture, and deployment of low-earth and medium-earth orbit communications satellites. Such cooperation would not only enhance Taiwan's C4ISR survivability and resilience against PLA threats but also strengthen supply chain security and bolster Taiwan's position as a key player.
- Advanced UAVs, such as the MQ-9, are welcome and much needed to support Taiwan's asymmetric warfare strategy. U.S. support in terms of the provision of data links, GPS navigation, and real-time intelligence is indispensable.

Autonomous-, cyber-, and space-related systems of the People's Republic of China (PRC) will play an important role in contributing to both gray-zone coercion and the warfighting threats confronting Taiwan and other like-minded regional partners across the entire spectrum of threat contingencies, from incursions to invasion. To that end, the PRC is most likely to resort to hybrid threats, such as cyber-electromagnetic operations to achieve cognitive effects or space-electromagnetic operations to disrupt and block Taiwan's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

To address these developments in more detail, this essay will provide a brief overview of China's cyber, space, and autonomous weapons developments and deployments that present the greatest threats to Taiwan's security, with a particular focus on an invasion scenario. The subsequent sections will consider Taiwan's responses, including its reckoning on recent developments in the Russia-Ukraine war, which are exemplary of the significance of emerging military operations across the domains, and options for Taiwan to more effectively partner with the United States to counteract PRC advances in the cyber, space, and autonomous realms.

Cyber- and Space-Related Threats

In the prelude to an invasion of Taiwan, the People's Liberation Army (PLA) Strategic Support Force is likely to perform gray-zone activities in the cyber-electronic space before the main body of PLA forces initiate a physical military invasion. The PRC will most likely initiate an advanced persistent threat (APT), ransomware attack, or a distributed denial of service (DDoS) flood to sabotage and stifle critical information infrastructure with the aim of disrupting the political and socioeconomic order in Taiwan. One oft-discussed PLA invasion scenario points to a power outage brought forth by cyberattacks around the afternoon tea break, the most inopportune moment before the end of the work and school day.

At the same time, the PRC would very likely initiate an APT attack on Taiwan's C4ISR apparatus, including sabotaging Taiwan's low-earth orbit and geosynchronous equatorial orbit communications satellites by infiltrating its satellite ground stations. With a temporary shutdown of certain parts of the C4ISR system, the reception of satellite images, and intelligence transmitted through communications satellites, the PLA will likely follow up with missile attacks upon the C4ISR network systems that the PLA Strategic Support Force and state-sponsored cyber mercenaries identify as remaining at work, having been recovered, or serving as backups.

While initial cyberattacks would cause power outages and traffic chaos, the PLA's kinetic missile attacks—with target acquisition powered by Gaofen-series reconnaissance satellites and navigation guided and timed by the BeiDou satellite system—will worsen the situation on the ground and lead to widespread fear and confusion. In the meantime, the PLA will selectively leave certain communication backbone networks functional to allow information, disinformation, and influence operations to convey images of climbing death tolls, horrifying damage, and, most importantly, panic. These kinds of operations will likely be waged and implemented throughout the whole process of the PLA invasion.

In later stages of the invasion, as soon as PLA weapon platforms leave coastal China bound for Taiwan and beyond, land-based backbone fiber cable and cell towers will no longer work effectively for PLA communications. As the PLA moves a greater distance from the mainland, most, if not all, navigation and communication will depend on satellite systems in space. The

PRC's BeiDou satellite system, coupled with Skylink tracking and data relay satellites and other communications satellite constellations capable of high-speed data transmission, will provide real-time communications as well as positioning, navigation, and timing capabilities for the PLA across a range of capabilities: missiles and hypersonic weapon platform attacks, air-sea battles during the blockades, air-sea-ground battles during the invasion of Taiwan, and air-sea battles in denying the U.S. military access between the first and second island chains.

Also critical at this stage of the invasion will be the use of weapons in and through space. The PRC's hypersonic glide vehicle, the equivalent of such repetitive-usable space weapons platforms as fractional orbital bombardment systems, aims to achieve a credible anti-access/area-denial deterrent through precision targeting and the possibility of carrying nuclear warheads. So far as the striking range is concerned, the PRC's hypersonic glide vehicle aims to strike targets beyond the Taiwan Strait, making Japan and the U.S. homeland vulnerable. In that light, whether North Korea's recent testing of a hypersonic weapon was technically supported by, and even transferred from, the PRC demands close attention.

Autonomous Weapons Threats

The PRC's autonomous weapons systems, whether aerial, sea surface/subsurface, or ground-based, are likely to be greatly enabled by the BeiDou navigation satellite system and Skylink tracking and data relay satellites. With Taiwan's potential "porcupine strategy" in mind, the PLA's remodeled, unmanned J-7 jet fighters will be part of an attrition strategy intended to wear down Taiwan's capabilities by gray-zone intrusion and harassment, consuming air-defense missiles as conflicts escalate. In addition, the PRC's anti-radiation unmanned aerial vehicles (UAVs) are meant to destroy Taiwan's C4ISR sensors and links in the first waves of attack.

The large GJ-11 stealth UAV, with the integration of surveillance and strike capabilities, coupled with the supersonic WZ-8 surveillance UAV and small-sized drone swarms, is likely to deliver decapitation operations and destruction of C4ISR systems, air-defense systems, airport runways, ports, and other critical military infrastructure. Surveillance-strike integration also allows the PLA's UAV loitering munition capabilities to shift to swarming attacks on Taiwan's key assets, including adversarial UAVs. CH-901 loitering UAVs, which resemble the U.S. Switchblade, are portable by either foot soldiers or tactical vehicles and can supposedly be deployed and catapult-launched within three minutes, thereby placing great pressure on an adversary's ground forces in urban battlefields. These loitering munitions present a high level of threat to Taiwan's air defense in that they are oftentimes flying low, slow, and even stealthily, making target acquisition a very difficult task.

UAVs capable of acting as communication relays would likely play a critical role in command and control during the PLA's beachhead landing and urban warfare. Given that satellite communication is liable to be periodically jammed, communication relay UAVs are of critical importance to PLA marine and army forces' WZ-10 attack helicopters and Z-20 utility helicopters once they depart from amphibious assault ships and fly toward targets in and around Taiwan. UAVs capable of communication relay ensure working datalinks among naval vessels at sea; helicopters, jet fighters, or reconnaissance planes in the air; and armored vehicles or tanks on the ground. Unlike the Skylink satellite system's provision of 5G-speed datalinks, the best speed and

volume of communication the PRC's UAVs can deliver is around 4G—and only when coupled with the deployment of ground cell towers.

Furthermore, the software-defined radio apparatuses installed in UAVs capable of communication relay allow for the creation of self-organizing networks and thereby possess counter-electromagnetic capabilities in defense of Taiwan's air-defense systems. With sufficient data collected from adversarial air-defense and electromagnetic equipment, AI-enabled algorithmic analytics are likely to boost the PLA's UAV counterstrike and attack capacity in the future. With the advancement of AI-enabled edge computing, surveillance-strike UAVs may carry out combat assessments, analyze campaign results in real time, and autonomously deliver follow-up strikes if necessary.

Taiwan's Response

Facing the PRC's powerful capabilities, Taiwan has embraced an overall defense concept (currently entitled "defense operations concept") to build and exercise asymmetric warfighting capabilities to thwart a PRC invasion.[1] In the buildup to a "fortress Taiwan" under a porcupine strategy, Taiwan's military services are to consolidate or build redundancy and resilience of C4ISR in both virtual and physical spaces.

To prepare for the worst-case scenario in which a large part of Taiwan's C4ISR is compromised or destroyed by PLA missiles or cyberattacks, the Ministry of National Defense has considered multiple countermeasures. UAV reconnaissance, UAV communication relay, and low-earth orbit communications satellites are within the capacity of Taiwan's defense industrial base to produce. In addition to procuring armed MQ-9 drones from the United States, Taiwan's National Chung-Shan Institute of Science and Technology (NCSIST) is developing several types of UAVs for reconnaissance and communication.[2] To build communication resilience, NCSIST has also developed mobile satellite communication ground vehicles in case satellite ground reception is compromised in the first wave of PLA kinetic and nonkinetic strikes.[3] Private companies collaborate with NCSIST in developing mobile radars and tracking systems to detect and block hostile UAVs. Building upon Taiwan's information and communications technology industrial capacity, Taiwan's private technology enterprises will likely play an important role in manufacturing satellite communications and reception components.

Furthermore, Taiwan has developed countermeasures against PLA satellite and UAV surveillance, including stealth and camouflage technology. Taking lessons from conflicts elsewhere in recent years, Taiwan's armed forces have devoted resources to develop and deploy counter-UAV measures, ranging from decoys, UAV identification friend or foe technology, point-defense phased-array radars, and radio frequency interference devices, most of which have been developed by either NCSIST or other domestic manufacturers. Among other countermeasures, NCSIST's CS/MPQ-90 phased-array radar systems have been deployed on outlying islands and on warships to detect UAVs.

---

[1] Ministry of National Defense (Taiwan), *ROC National Defense Report 2021* (Taipei, November 2021), 59.

[2] "Aviation Systems," National Chung-Shan Institute of Science and Technology (NCSIST), https://www.ncsist.org.tw/eng/csistdup/products/products.aspx?catelog_Id=9.

[3] "Satcom on the Move," NCSIST, https://www.ncsist.org.tw/eng/csistdup/products/product.aspx?product_id=75&catalog=11.

Following the path of the U.S. Cyber Command, Taiwan's cyber forces intend to adopt "defending forward" guidelines without breaching international laws, norms, or civil rights.[4] Moreover, drawing on certain lessons learned regarding the dubious borderline issues in cyberwarfare, Taiwan's government is taking seriously the feasibility of the extant on-the-ground rules of engagement for its cyber forces. Critical to the growth of Taiwan's cyberoperation capabilities are talent recruitment, training, and retention, with the Ministry of National Defense taking notes from Israel's talent-tailored recruitment and reserve system.

Going beyond cybersecurity, Taiwan has adopted a whole-of-government approach to tackle information security issues for the protection of hardware and software throughout the supply chain of its defense industrial base. In addition, to materialize the Fortress Taiwan concept, the country's armed forces have begun to introduce further passive defenses for hardware storage and backup in underground strongholds to counter electromagnetic pulse threats posed by the PLA. Moreover, NCSIST has developed mobile ground vehicles for electromagnetic interception, acquisition, direction finding, and jamming to support Taiwan's electronic warfare needs.[5]

In addition to conducting a firm defense, the other side of Taiwan's defense operations concept looks to expand defensive space, aiming to force the enemy to assemble forces at airfields or ports farther away from areas opposite Taiwan, ultimately enhancing multidomain deterrence. Strike capabilities are therefore sought, including the acquisition of standoff strike weapons, electronic warfare pods, and MS-110 reconnaissance pods for Taiwan's upgraded F-16s. Furthermore, Taiwan's armed forces have developed the Chien Hsiang anti-radiation UAVs and the aforementioned forward-defending cyberstrike capabilities.[6]

Early Lessons Learned from the Russia-Ukraine War

Domestic Concerns

While a consensus has emerged in Taiwan that asymmetric warfighting capabilities are imperative, there has been no conclusive direction regarding the way forward. Many perceive intraservice competitions and partisan rivalries as normal in almost every consolidated democracy. Yet Taiwan is the only democracy under a present and imminent military threat posed by China. What is worse is that time is not on Taiwan's side. China has accelerated its military modernization in every domain, with salient progress on cyber, space, and autonomous weapons.

Oftentimes, intraservice debates within the barracks make media headlines, leading to congressional interpellations, or vice versa, and creating bumps on the road toward Taiwan's porcupine strategy. One case that has raised many eyebrows is Taiwan's decision to procure U.S. M1A2 main battle tanks at a time when the U.S. Army, followed by the U.S. Marines, is abandoning them. One counterargument in Taiwan is that these tanks are essential to oppose PLA tanks during the amphibious landing and, after that, to offer cover for foot soldiers in the urban battlefields.

---

4 Ministry of National Defense (Taiwan), *ROC National Defense Report 2021*, 59, 73.

5 "Interception, Acquisition, Direction Finding and Jamming Vehicle," NCSIST, https://www.ncsist.org.tw/eng/csistdup/products/product.aspx?product_Id=74&catalog=11.

6 Ministry of National Defense (Taiwan), *ROC National Defense Report 2021*, 59, 60, 67, 69, 73.

Reckonings in Taiwan

The events unfolding in the ongoing Russia-Ukraine war that started on February 24, 2022, have unexpectedly straightened (or focused) Taiwan's course on the path toward building a Fortress Taiwan. Witnessing Ukrainians' use of precision weapons, such as the land-based Neptune and portable Stinger and Javelin missiles, to sink Russian naval battleships, shoot down jet fighters and helicopters, and crush tanks and armored vehicles, has not only confirmed Taiwan's roadmap to asymmetric warfighting but also served as a reckoning on calls for the procurement of a large stockpile of light, mobile, and precise weapons instead of large, expensive, and sophisticated weapon platforms. Additional lessons Taiwan has drawn from the ongoing war in Ukraine range across the spectrum of cyber, electronic warfare, space, and autonomous weapons, as well as cognitive operations and military training.

Yet most, if not all, defense experts in Taiwan agree—and they even had to articulate this point at the beginning of the war in Ukraine—that Taiwan's case is nowhere close to that of Ukraine. There is no such thing as "Ukraine today, Taiwan tomorrow." Extensive discussions of the abovementioned issues are ongoing at the time of writing, as are various wargaming and tabletop exercises, all toward the goal of drawing on the lessons learned; discerning what does and does not fit Taiwan's case; identifying the current state of the China threat, the requirements to counter it, and the gaps in between; and then mapping the steps to move forward. Below is a brief analysis illuminating several early takeaways and reckonings from Taiwan's perspective.

Resilience matters. First and foremost, resilience matters across physical and virtual spaces in different domains, and the buildup of resilience takes time and cannot be achieved overnight. In the cyber domain, the internet remains at work in Ukraine, to almost everyone's surprise. But that by no means indicates that Russia did nothing in cyberspace to disrupt Ukraine's internet and communications. On the eve of the war, Russia launched not just DDoS attacks on Ukrainian government systems but also malicious attacks on GPS and communications satellite systems to cut off data links and navigation capabilities that might assist the Ukrainian resistance.

Ukraine, under fierce cyberattacks by Russia since 2014, holds no illusions about keeping the internet intact and safe from disruptions. Instead, Ukraine has been redirecting the internet routes and establishing measures to save, repair, and restore data, links, and backbone fiber cables; build multiple communication channels; prepare for emergency communication networks; and cultivate voluntary white-hat hackers ready for quick response, rescue, and retaliation against adversarial hacking. Despite the internet being either stymied by DDoS attacks launched by Russian state-sponsored and pro-Russian nationalist hackers or cut off by artillery shelling of backbone fiber networks, Ukraine strived to repair and restore the backbone links to keep delivering messages with battlefield images and cognitive/psychological campaigns to the outside world. These efforts have been aided by SpaceX commercial communications satellites and reception depots.

The success of Ukrainian endeavors in cyber and communication resilience has been inspiring for Taiwan. Just as Russia uses Ukraine as a testing bed for cyberoperations and influence campaigns, Taiwan has experienced China's intensive cyber and online cognitive operations for years. Suffice to say, Taiwan is better prepared for cyberoperations than Ukraine since its Cyber Command has been in the order of battle since 2017 and has received intensive attention and resources from Taiwan's civilian presidents. In addition, the command has been drawing pragmatic lessons from Israel's success story in recruiting, retaining, and collaborating with civilian talent.

Differences in the cyber domain. That said, several differences make Taiwan a distinct case from Ukraine if the PLA tries to disconnect its communications links to the outside world. For one, certain countermeasures taken by Ukraine in the cyber domain might give Taiwan pause. Calls for the weaponization of the Domain Name System (DNS), for instance, are not an option for Taiwan. However, calling for global hacktivists, such as Anonymous, to be involved in the country's defense is something it would definitely try—if the connected undersea cables and four land-based reception stations remain intact and functional.

Unlike Ukraine, which has land borders with neighboring states and is connected via land-based backbone fiber cable networks, Taiwan is surrounded by oceans and must rely on undersea cables and satellites. Importantly, repairing cable networks is much easier and quicker on land, thereby raising the likelihood that Taiwan would require outside support. Hence, Taiwan has taken this resilience issue seriously and is working on solutions such as building its own cable repair ships to shorten the time needed for restoration.

One of the keys to effective communication and cyber resilience is establishing multiple channels for redundancy. The Ukrainian lesson is likely to accelerate Taiwan's efforts to rapidly deploy and install multiple communications satellite networks in the space domain during peacetime. Yet, this goes way beyond many small powers' capabilities to build their own military communications satellite constellations, and Taiwan is no exception. A feasible option, based on the Ukraine case again, would be to resort to collaboration with like-minded regimes to deploy a hybrid of at least three geosynchronous equatorial orbit military communications satellites with multiple amplifiers and receptors for a couple of frequency bands together with a number of medium-earth and low-earth orbit commercial communications satellites.

Outside support. Ways of seeking outside support would be another salient difference between Taiwan and Ukraine. Delivery of SpaceX satellite reception depots to Ukraine under contingency conditions, for instance, requires ground transportation across borderlines from Poland, whereas a delivery of the kind would be problematic and risky, if not impossible, during a PLA blockade of the waters surrounding and air space over Taiwan. Given that reasonably likely scenario, Taiwan is considering potential measures to store sufficient critical materials, parts, and equipment at multiple underground warehouses on and around the island.

The next takeaway concerns how and what Taiwan needs to seek outside support. For sure, some of the great performances made by Ukrainian noncommissioned officers, special operations enabled by electronic warfare, and psychological operations (PSYOPS), as well as the effective use of drones, are the accumulation of long-term outside support through collaborative training, trust building, and numerous joint exercises. In a nutshell, Taiwan is moving in the right direction in this regard.

Procurement, storage, and deployment. In addition, with the success of Ukrainian forces in sinking Russian naval warships, Taiwan has learned that it is on the right track of increasing the procurement, storage, and deployment of anti-ship cruise missiles, land-based mobile anti-ship cruise missile platforms and their corresponding mobile radar surveillance, microwave communications, and decoy platforms. What might need to be done rather quickly is to manufacture, procure from abroad, and safely stockpile a number of small, portable anti-tank Javelin and air-defense Stinger missiles, which would be valuable in coastal defense, the defense of military facilities, and urban warfare.

Indigenous development of UAVs. The impressive performance of the Ukrainian military and civilian UAVs, capable of surveillance, identification, locating, navigating, or delivering strike munitions, provides ample justification for Taiwan's indigenous development of UAVs. NCSIST and its satellite suppliers have drawn much attention to specific lessons Taiwan may derive from Ukraine's recent utilization of TB-2 and civilian UAVs, whether they are drones serving as decoys to distract attention from Russian warships or platforms offering real-time location data for precision strikes on tank battalions. However, the data link, UAV signal integration platform, and real-time intelligence sharing by NATO member states, altogether rendering an enhanced level of battlefield management, have generated a mixed sense of high hope and uncertainty in Taiwan's armed forces. While UAVs have become a buzzword in Taiwan's armed forces, particularly among the ground forces and marines, only a limited number of U.S. MQ-9 and NCSIST drones of varying sizes, with some space for future improvement, are at their disposal. Moreover, whether and in what ways battlefield intelligence surrounding Taiwan might be shared in real-time fashion remain uncertain.

Conclusion: Ways Forward for Partnering with the United States

An interoperable communications system is the first and foremost priority for the U.S.-Taiwan partnership to counter the PRC's autonomous weapons, cyber, and space threats. It will be critical for the United States and Taiwan to gradually establish an integrated, cross-domain, common operational picture. In the meantime, much work is needed in bilateral and multilateral closed-door wargaming, nondisclosed military exercises, mutual understanding of rules of engagement, trust building, and counterintelligence efforts. Semi-annual Track 1.5 tabletop exercises hosted by think tanks may serve as a good option for experimenting with cooperative security concepts never before put to test.

To fill this gap in a timely manner, several interim steps are imperative. First, cyber forces, joined by benign civilian hackers, in the United States and Taiwan should work together to exchange notes on rules of engagement to develop a coordinated emergency plan. This is critical, as the breakdown of either the power grid or the internet network, or both, is highly likely to occur before the PLA launches its first wave of kinetic attacks. Expanding the parameters for U.S.-Taiwan cybersecurity collaboration is equally important. Building on the long-standing collaborations on defense readiness and frequent calls for visits between the U.S. and Taiwan cybersecurity communities, it is time for both sides to draw on lessons learned in Ukraine and figure out ways for synchronized or coordinated forward defense in cyberspace.

It is also essential for Taiwan to keep up with the fast pace of information operations, particularly with regard to the effective delivery of precise and correct messages to the population in the absence of, or with the limited provision of, electric power and internet connections. Training in information operations, particularly PSYOPS, would greatly assist Taiwan's special operations forces, reserve forces, and political warfare officers. Taiwan's special operations forces, together with the Political Warfare Department's PSYOPS platoon and the Cyber Command's PSYOPS units, could all benefit from the training sessions and workshops the U.S. military provides in the United States and Taiwan.

Moreover, as illuminated in the case of the Russia-Ukraine war, redundant UAV capability is needed for the continuity of aerial surveillance in the aftermath of PLA kinetic strikes and

cyberattacks, which will also likely target Taiwan's small number of MQ-9 drones. Along this line, more advanced UAVs, such as the MQ-9, are welcome and much needed to support Taiwan's asymmetric warfare strategy. U.S. support in terms of the provision of data links, GPS navigation, and real-time intelligence is indispensable. Given that Taiwan will likely be under a PLA air-sea blockade, advanced large-sized UAVs deployed and stored near the island are important because they will be more capable of penetrating through the access-denial layers installed by the PLA.

Deploying counterspace weapons in order to defend against threats posed by missiles, hypersonic weapons, and space surveillance is currently beyond Taiwan's capacity—and is also at odds with its asymmetric warfare strategy. To build countermeasures, the United States should deploy detection and early-warning sensors in Taiwan and other like-minded allies and partners in the Indo-Pacific, as well as share data and intelligence in real-time. It is appropriate for Taiwan to fairly share the costs of the device- or service-related R&D and maintenance as long as it participates in and benefits from the awareness-building and intelligence collaborations.

Last, but by no means least, the United States should collaborate more closely with Taiwan's advanced information technology industry in the development, manufacture, and deployment of medium-earth and low-earth orbit communications satellites. Such cooperation will not only enhance Taiwan's C4ISR survivability and resilience against PLA threats but also strengthen supply chain security and bolster Taiwan's position as a key player in future satellite operation collaborations. In the meantime, Taiwan must have a compatible information security apparatus in place to protect the data flow and business secrets across its defense industrial bases. Counterintelligence measures, including those conducted by military units, are already at work, and more measures, such as closely following the U.S. Department of Defense's Cybersecurity Maturity Model Certification, are on the way.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

China's Cyber, Space, and Autonomous Weapons Systems: India's Concerns and Responses

Rajeswari (Raji) Pillai Rajagopalan

RAJESWARI (RAJI) PILLAI RAJAGOPALAN is the Director of the Centre for Security, Strategy and Technology at the Observer Research Foundation (ORF) in New Delhi. She can be reached at <rpr@orfonline.org> or on Twitter <@raji143>.

EXECUTIVE SUMMARY

This essay examines India's key concerns about China's growing technological prowess in the areas of cyberspace, outer space, and artificial intelligence and automation; the Indian response; and the potential for India and the U.S. to collaborate on these strategic technologies.

MAIN ARGUMENT

China has made significant technological gains, especially in the area of critical and emerging technologies, such as outer space, cyberspace, and autonomous weapons. Its attempts to gain parity with the U.S. have had the net effect of creating a military force that is technologically far superior to India's. This technological prowess has the potential to make Indian efforts at countering China a lot more challenging, and even broaden the power asymmetry between the two countries. As China gains greater proficiency in these technologies in relation to India, it also makes New Delhi's deterrence calculations a lot riskier. China's growing cyber capabilities include the ability to undertake influence and information operations as well as offensive cyber tools with the capability to strike the critical infrastructure of its adversaries. Similarly, China's growing array of counterspace capabilities, including anti-satellite weapons and cyber and electronic warfare, have consequences for India. China's advancements in artificial intelligence and automation with military applications are also of consequence. In sum, China's growing technological proficiencies, along with its aggressive behavior, have forced India to respond. The Indian response has involved capability development, changes in policy, and institutional innovation. India has also accelerated its strategic partnership with the U.S. and other partners in Asia, including Japan, Australia, and France.

POLICY IMPLICATIONS

- China's technological advances will potentially make India's deterrence strategy less effective.
- China's growing proficiency in critical and emerging technologies increases the likelihood of a destabilizing arms race in the region and beyond.
- China's growing technological competencies and India's responses will likely require greater collaboration between India and its partners, including the U.S. as well as Japan, Australia, and France.

The People's Republic of China (PRC) has made numerous noteworthy technological advancements in critical and emerging technologies such as outer space, cyberspace, quantum, and autonomous weapons. Though China may have developed these technologies in response to U.S. power, they nevertheless have security implications for India. The development of these capabilities by China could potentially make India's efforts to deter any attacks more problematic, and it could further increase the power gap between the two countries. The stronger China becomes relative to India, the more difficult it becomes for India to exercise its deterrence strategy. Another key problem is that many of these new technologies and weapons can increase the potential for surprise attacks, potentially leading to a destabilizing arms race spiral between key great powers in the region, all of whom are working on developing these weapons.

This essay outlines New Delhi's key concerns about China's critical and emerging technologies, as expressed by the Indian government or by Indian security analysts. It then discusses India's response to these concerns and considers the potential for greater U.S.-India cooperation in these areas.

Indian Concerns

The PRC's Cyber Capabilities

China's growing cyber capabilities range from influence and information operations to offensive cyber tools capable of targeting its adversaries' critical infrastructure. Even if China does not have a cyberwarfare doctrine, it still possesses an offensive cyber capability for reconnaissance, attack, defense, and deterrence.[1]

There have been many cyberattacks on India that, based on the addresses of the computers, appear to have originated from various countries, including China.[2] Though the Indian government is careful about not identifying China, Rajeev Chandrasekhar, the minister of state for electronics and information technology, stated that according to the Indian Computer Emergency Response Team (CERT-In), the total number of attacks had gone up from 394,499 in 2019 to 1,402,809 cybersecurity incidents in 2021 and 674,021 in the first half of 2022 (January–June 2022).[3] It is difficult to obtain official confirmation of specific events, but there are growing concerns about China's use of cyberwarfare to penalize India by imposing economic and security costs on the country. For example, in October 2020, Maharashtra, a western Indian state, experienced a power outage of several hours. The state's energy minister, Nitin Raut, said it was an act of "sabotage." The central government in New Delhi has not identified the source of the attack, but there is widespread suspicion that it originated in China.

Other reporting also points to China. According to one analysis, China has been "launching cyberattacks that may have caused blackouts across India."[4] Additionally, according to one report from Recorded Future, a U.S.-based cybersecurity firm, "Chinese malware was flowing into the

---

[1] "Cyber Capabilities and National Power: A Net Assessment," International Institute for Strategic Studies (IISS), June 2021, 97, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[2] Ministry of Electronics and Information Technology (India), "Lok Sabha Unstarred Question No. 2719: Cyber Attacks," August 4, 2021, http://164.100.24.220/loksabhaquestions/annex/176/AU2719.pdf.

[3] Ministry of Electronics and Information Technology (India), "Lok Sabha Unstarred Question No. 1553: Cyber Security Incidents," July 28, 2021, http://164.100.24.220/loksabhaquestions/annex/176/AU1553.pdf; and Ministry of Electronics and Information Technology (India), "Lok Sabha Unstarred Question No. 1743: Cyber Attacks," July 27, 2022, http://164.100.24.220/loksabhaquestions/annex/179/AU1743.pdf.

[4] U.S.-China Economic and Security Review Commission, "2021 Report to Congress of the U.S.-China Economic and Security Review Commission," November 2021, https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf.

control systems that manage electric supply across India, along with a high-voltage transmission substation and a coal-fired power plant," though "most of the malware was never activated."[5] Stuart Solomon, chief operating officer of Recorded Future, noted that a Chinese state-sponsored group has "systematically utilize[d] advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure."[6] Thus, despite the Indian government's reluctance to identify China, there is credible suspicion of Chinese cyberattacks on India.

There could be multiple reasons why India is reluctant to name China. One is that, with the ongoing tensions between them, New Delhi does not want to make the situation worse. Second, India possibly does not want to reveal how it identified the source of the attack, especially if the identification was done in collaboration with other friendly governments. Third, it is also possible that India does not have the technical expertise to identify with certainty that China was the source of the attack. Finally, India might not see much point in identifying the source if it does not have sufficient means to retaliate.

The PRC's Space Capabilities

China's advancing space capabilities have been of concern to Indian security managers because of India's increasing employment of its space capabilities for both developmental and military purposes. China's first successful anti-satellite (ASAT) test in January 2007 was a wake-up call for India, kickstarting a new debate within India on the threats, challenges, and ways to deter and protect its space assets. It forced India to re-evaluate its traditional policy against space militarization and created incentives for the country to develop its own ASAT capability to defend itself from Chinese threats.

The threat is significant. ASAT weapons have the potential to disable GPS satellites, which could affect some targeting and navigation systems.[7] Similarly, Indian foreign minister Pranab Mukherjee indicated that China's space capability poses a strategic challenge, saying that India "would need to develop more sophisticated ways of dealing with these new challenges posed by China."[8] Indian defense minister A.K. Antony expressed similar concerns when establishing the Integrated Space Cell at the Integrated Defence Services Headquarters. While not calling out China by name, he commented on "the growing threat" to Indian space assets in the neighborhood, saying that "offensive counter-space systems like anti-satellite weaponry, new classes of heavy-lift and small boosters and an improved array of military space systems have emerged in our neighborhood."[9]

China's counterspace capabilities include direct-ascent ASAT weapons, high-powered lasers, co-orbital satellites, directed energy weapons, electronic jamming and spoofing, and cyber means that have been developed over the past decade. There are a growing number of instances in which

---

[5] David E. Sanger and Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *New York Times*, February 28, 2021, updated September 27, 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html.

[6] Ibid.

[7] "India to Counter China's Anti-satellite Test, Says DRDO," *Tribune*, January 21, 2007.

[8] Pranab Mukherjee, "Address by Mr. Pranab Mukherjee, Hon'ble Minister for External Affairs at National Defence College, New Delhi, 3rd November, 2008 India's Security Challenges and Foreign Policy Imperatives," Ministry of External Affairs (India), November 3, 2008, https://mea.gov.in/Speeches-Statements.htm?dtl/1767/Address+by+Mr+Pranab+Muk; and "Address by NSA at the 9th IISS Asia Security Summit," Ministry of External Affairs (India), June 5, 2010, https://www.mea.gov.in/in-focus-article.htm?661/Address+by+NSA+at+the+9th+IISS+Asia+Security+Summit.

[9] Sudha Ramachandran, "India Goes to War in Space," *Asia Times*, June 18, 2008, https://web.archive.org/web/20081203131949/http://www.atimes.com/atimes/South_Asia/JF18Df01.html.

China has employed these capabilities against U.S. space assets.[10] Technologies that China is developing or has developed, including active debris removal and on-orbit satellite servicing, are likely to increase Indian concerns. Finally, China's institutional innovations, such as the creation of the People's Liberation Army (PLA) Strategic Support Force and the integration of space, cyber, and electronic warfare, suggest that China has much bigger and more ambitious plans for its military space program.[11]

The PRC's Autonomous Weapons Capabilities

China's advances in artificial intelligence (AI) and automation with applications in the military arena could have implications for India. According to the 2019 Chinese defense white paper, "intelligent warfare is on the horizon," and China needs to "speed up the development of intelligent military."[12]

Indian analysts write that China's focus on intelligentized warfare "enables 'shortened' high 'tempo,' 'accurate' operations, reducing the length of what one Chinese military strategist called 'observation-judgment-decision-action.'"[13] As one Indian scholar put it, "China has created an aura of being the undisputed military leader in key AI related military technologies with a deterrence logic of its own."[14] Indian analysts suggest that with greater AI infusion into the PLA's military platforms, "the PRC and the PLA have moved away from attrition-type warfare involving debilitating mass attacks that cause heavy casualties, to non-contact warfare involving long-distance and standoff range delivery of accurate and lethal firepower that enables the PLA to secure a quick, low-cost and decisive victory."[15]

China's AI applications in its military platforms will also significantly affect Indian security. For instance, large numbers of aging Chinese battle tanks such as the Type 59 are reportedly being converted to unmanned systems that can be fielded on the Ladakh plateau.[16] The PLA's focus on unmanned ground vehicles for logistics purposes could also have relevance for India.[17] Similarly, China has been making efforts over the last five to six years to develop drone swarms that can operate autonomously. Indian analysts worry that this may be "the most effective use of

---

[10] Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space," UN Institute for Disarmament Research, Space Dossier, no. 3, May 2019, https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

[11] Taylor A. Lee and Peter W. Singer, "China's Space Program Is More Military Than You Might Think," Defense One, July 16, 2021, https://www.defenseone.com/ideas/2021/07/chinas-space-program-more-military-you-might-think/183790; and Mark Stokes et al., "China's Space and Counterspace Capabilities and Activities," U.S.-China Economic and Security Review Commission, March 30, 2020, https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf.

[12] State Council Information Office of the People's Republic of China (PRC), *China's National Defense in the New Era* (Beijing, July 2019), https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

[13] Kartik Bommakanti, "A.I. in the Chinese Military: Current Initiatives and the Implications for India," Observer Research Foundation (ORF), Occasional Paper, no. 234, February 2020, https://www.orfonline.org/wp-content/uploads/2020/02/ORF_OccasionalPaper_234_AI-ChineseMilitary.pdf.

[14] Surjeet Singh Tanwar, "Artificial Intelligence in Military: Evolving Battlespace and Warfighting of 21st Century," Centre for Land Warfare Studies, Issue Brief, no. 278, March 2021, https://www.claws.in/static/IB-278_Artificial-Intelligence-in-Military-Evolving-Battlespace-and-Warfighting-of-21st-Century.pdf.

[15] Bommakanti, "A.I. in the Chinese Military."

[16] "How China Is Using AI to Turn its Massive Type 59 Tank Divisions into an Army of Lethal Combat Robots," *Military Watch*, April 5, 2021, https://militarywatchmagazine.com/article/how-china-is-using-ai-to-turn-its-massive-type-59-tank-divisions-into-an-army-of-lethal-combat-robots; and Asia Times, "China Is Turning Old Tanks into AI-Equipped Robots," *National Interest*, May 9, 2018, https://nationalinterest.org/blog/the-buzz/china-turning-old-tanks-ai-equipped-robots-25753.

[17] Elsa B. Kania, "'AI Weapons' in Chinese Military Innovation," Brookings Institution, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania.pdf.

AI weapons technology."[18] The PLA Navy is also exploring unmanned surface vessels that could possibly "operate with some autonomy" and may be developing autonomous submarines.[19]

Reports also suggest China has been investing in "large, smart and relatively low-cost unmanned submarines" that can undertake a number of missions, including reconnaissance, mine placement, or even self-destructive missions while targeting enemy ships.[20] These vessels are expected to be inducted into service in the early 2020s. Reports further indicate that China has been involved in developing autonomous underwater vehicle projects in addition to unmanned underwater vehicles.[21] Indian naval analysts are also concerned about China's efforts at developing an "underwater Great Wall" of seabed sensors. China's efforts in this regard have been particularly concerning to the Indian naval establishment.[22]

Additionally, the PLA Air Force already flies advanced unmanned systems that can operate with limited autonomy, but experts suggest that these systems could be enhanced further to make them more autonomous.[23] Experts are also of the view that the PLA Strategic Support Force could apply AI to areas like space, cyber, electronic, and psychological warfare. For instance, on the space front, Chinese scientists claimed earlier in 2022 that they had successfully tested an anti-satellite AI system to attack a target satellite in a simulated space battle. A team of scientists, including Dang Zhaohui, a professor of astronautics at Northwestern Polytechnical University, has repeatedly experimented using an AI system to command three small hunter satellites to seize "a high-value target" in space.[24] Similarly, the Chinese military has plans to use big-data analytics, machine learning, and automation "to enhance the defense of critical military and civilian networks and scale the effects of offensive cyber operations." China also believes that by using technologies such as pattern recognition and deep learning, "AI can not only be helpful for detecting the vulnerability of enemies' networks but can also assist the protection of friendly systems by detecting loopholes that need to be fixed."[25] Similarly, the Chinese military's efforts to use AI technologies in the jamming, blinding, or hacking of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems are noteworthy.[26]

---

18 Bedavyasa Mohanty, "Lethal Autonomous Dragon: China's Approach to Artificial Intelligence Weapons," ORF, November 15, 2017, https://www.orfonline.org/expert-speak/lethal-autonomous-weapons-dragon-china-approach-artificial-intelligence.

19 Kania, "'AI Weapons' in Chinese Military Innovation"; Thomas Newdick, "China Tested an AI-Controlled Submarine-Hunting Underwater Drone a Decade Ago: Report," War Zone, July 9, 2021, https://www.thedrive.com/the-war-zone/41478/china-tested-an-ai-controlled-submarine-hunting-underwater-drone-a-decade-ago-report; and David Hambling, "China's New Unmanned Attack Sub May Not Be What It Seems (Update: In Fact It's a Paper Tiger)," *Forbes*, July 9, 2021, https://www.forbes.com/sites/davidhambling/2021/07/09/chinas-new-unmanned-attack-sub-may-not-be-what-it-seems/?sh=221c54d03658.

20 Stephen Chen, "China Military Develops Robotic Submarines to Launch a New Era of Sea Power," *South China Morning Post*, July 22, 2018, https://www.scmp.com/news/china/society/article/2156361/china-developing-unmanned-ai-submarines-launch-new-era-sea-power?module=perpetual_scroll_0&pgtype=article&campaign=2156361.

21 Ryan Fedasiuk, "Leviathan Wakes: China's Growing Fleet of Autonomous Undersea Vehicles," Center for International Maritime Security, August 17, 2021, https://cimsec.org/leviathan-wakes-chinas-growing-fleet-of-autonomous-undersea-vehicles.

22 "India Gearing to Develop Use of Unmanned Underwater Vehicle (UUV)," Prasar Bharati, July 28, 2021, https://newsonair.com/2021/07/28/india-gearing-to-develop-use-of-unmanned-underwater-vehicle-uuv; and Abhijit Singh, "How India, Too, Is on a Quest for Undersea Dominance, to Counter the Chinese Navy's Growing Presence," ORF, August 31, 2018, https://www.orfonline.org/research/43742-how-india-too-is-on-a-quest-for-undersea-dominance-to-counter-the-chinese-navys-growing-presence.

23 Kania, "'AI Weapons' in Chinese Military Innovation."

24 Gabriel Honrada, "China Uses AI Deception in Simulated Space Battle," *Asia Times*, June 16, 2022, https://asiatimes.com/2022/06/china-uses-ai-deception-in-simulated-space-battle.

25 Jiayu Zhang, "China's Military Employment of Artificial Intelligence and Its Security Implications," *International Affairs Review*, August 16, 2022, https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap.

26 Ryan Fedasiuk, "China Invests in Artificial Intelligence to Counter U.S. Joint Warfighting Concept: Records," Breaking Defense, November 10, 2021, https://breakingdefense.com/2021/11/china-invests-in-artificial-intelligence-to-counter-us-joint-warfighting-concept-records.

Indian Responses

India's continuing problems with China on the Sino-Indian border and elsewhere have brought home the bitter reality that it must respond to the growing technological asymmetry between the two countries. The asymmetry in key technology areas like cyber, space, and autonomous weapons has given China a remarkable advantage that could tilt the military balance.

Cyber Capabilities

India has been cognizant of various threats in the cybersecurity realm and is expanding its measures to prevent cyberattacks on critical infrastructure. Following isolated incidents on vital installations, such as the attack on the administrative network of the Kudankulam Nuclear Power Plant in 2019, the government undertook a series of steps to address the gaps.

Following this cyberattack, as well as one on the Indian Space Research Organisation, questions were raised in Parliament about whether the defense sector had faced any cyberattacks and if there were gaps in the security of the military's covert and sensitive information. The minister of state for defence revealed that the "government has approved establishment of [the] Defence Cyber Agency to control and coordinate the Joint Cyber operations…To mitigate cyber threats, all the three Services have established their respective Cyber Emergency Response Teams (CERT)."[27] The government also established the around-the-clock Security Monitoring Centre at the National Informatics Centre (NIC) "for detecting and responding to security incidents related to NIC infrastructure and data centres."[28] According to the minister of state for defence, the government is in the final stages of formulating a national cybersecurity strategy, which could help conceptualize what India might require in terms of cyberwarfare capabilities.[29]

With regard to the growing cyberthreats to India from China and other adversaries, the government has taken a number of measures "to enhance the cyber security posture and prevent cyberattacks."[30] These include CERT-In issuing alerts and advisories for the latest cyberthreats and vulnerabilities as well as countermeasures to secure hardware, networks, and data; CERT-In sending early-warning threat intelligence alerts to more than seven hundred organizations across multiple sectors; the government providing advisories for chief information security officers on their key roles and responsibilities to protect applications and infrastructure as well as to ensure compliance; and security audits to ensure compliance with information security best practices.[31] More importantly, the government has been conducting cybersecurity mock drills and exercises in order to assess the posture and preparedness of various institutions of the government as well as critical sectors.[32]

In addition, the Information Technology Act mandated the establishment of the National Critical Information Infrastructure Protection Centre, which is the national nodal agency for critical information infrastructure protection. The government has also established the National

---

27 Ministry of Defence (India), "Lok Sabha Unstarred Question No. 642: Cyber Security of Defence Network," November 20, 2019, http://164.100.24.220/loksabhaquestions/annex/172/AU642.pdf.

28 Ministry of Electronic and Information Technology (India), "Lok Sabha Unstarred Question No. 1412: Cyber Attack on Critical Infrastructure," July 28, 2021, http://164.100.24.220/loksabhaquestions/annex/176/AU1412.pdf.

29 Ministry of Defence (India), "Lok Sabha Unstarred Question No. 2532: Cyber Warfare," August 4, 2021, http://164.100.24.220/loksabhaquestions/annex/176/AU2532.pdf.

30 Ministry of Electronics and Information Technology (India), "Lok Sabha Unstarred Question No. 1553: Cyber Security Incidents."

31 Ibid.

32 Ibid.

Cyber Coordination Centre to create appropriate levels of situational awareness of currently prevalent and potential cybersecurity threats. Furthermore, the government has set up a cyber crisis management plan to respond to cyberattacks and cyberterrorism, which is to be implemented by all ministries and departments, as well as by state governments and critical sectors. Almost all the Indian actions are reactive in nature, responding to threats and incidents. For India to effectively address the growing Chinese threats in the cybersecurity domain, it needs to prioritize the development of cyberwarfare capabilities. This could be done by India on its own as well as in coordination with strategic partners, including the United States, Japan, and Australia.

Space Prowess

India's response to China's growing space capabilities has been most evident with regard to ASAT weapons and other counterspace capabilities. India's Mission Shakti ASAT test in March 2019 was its response to China's ASAT weapons and signaled that India has the capability to disrupt and damage China's space assets if Beijing carries out strikes. Furthermore, in response to China's growing counterspace capabilities, Satheesh Reddy, the head of the Defence Research and Development Organisation (DRDO), said that India is working on a range of counterspace capabilities, including "directed energy weapons (DEWS), lasers, EMP and co-orbital killers as well as the ability to protect its own satellites from electronic or physical attacks."[33]

In addition to developing its capabilities, India has responded by establishing new institutions that can address the growing Chinese space threats. Following China's ASAT test, India announced in 2010 the establishment of the Integrated Space Cell under the Integrated Defence Services headquarters of the Indian Ministry of Defence in order to more effectively streamline the utilization of space for military and broader security purposes. Moreover, India in 2019 conducted its first space security wargame, called IndSpaceEx. The exercise included the participation of the military and the scientific establishment, which was an indication of the maturing synergy between key stakeholders.[34] India's creation of the Defence Space Agency in 2019 is also remarkable in this context.

Autonomous Weapons Capabilities

China's focused attention on AI and autonomous weapons has begun to appear on the radar of the Indian establishment. In 2018 the defence production secretary stated that going forward, AI will be integrated as an important aspect of the Indian military to augment the "operational preparedness of the armed forces in a significant way that would include equipping them with unmanned tanks, vessels, aerial vehicles and robotic weaponry."[35] This reportedly fits into a broader government strategy "to prepare the Army, Navy and the Air Force for next generation warfare and comes amid rising Chinese investments in developing critical applications of AI for its military."[36] Meanwhile, the DRDO said that it is taking a "proactive approach" to make sure

---

33 Rajat Pandit, "India to Hold First Simulated Space Warfare Exercise Next Month," *Times of India*, June 8, 2019, https://timesofindia.indiatimes.com/india/india-to-hold-first-simulated-space-warfare-exercise-next-month/articleshow/69697289.cms.

34 Rajeswari Pillai Rajagopalan, "A First: India to Launch First Simulated Space Warfare Exercise," *Diplomat*, June 12, 2019, https://thediplomat.com/2019/06/a-first-india-to-launch-first-simulated-space-warfare-exercise.

35 "India Working on Unmanned Tanks, Vessels, Robotic Weaponry for Future Wars," Press Trust of India (PTI), May 20, 2018, available at https://timesofindia.indiatimes.com/india/india-working-on-unmanned-tanks-vessels-robotic-weaponry-for-future-wars/articleshow/64243702.cms.

36 "India Working on Artificial Intelligence to Prepare Armed Forces for Next-Gen Warfare," PTI, May 20, 2018, https://www.hindustantimes.com/india-news/india-working-on-unmanned-tanks-vessels-robotic-weaponry-for-future-wars/story-u6GyiMWkX7OObwoPJ2pXXL.html.

that India has the capability for "artificial intelligence–based systems including the command-and-control system."[37] The goal is to shift from a manpower-intensive to a technology-aided force to meet the emerging security challenges, but there is a yawning gap between these stated goals and the acquisition trajectory. However, some analysts believe that India is "not far behind," pointing to the November 2021 demonstration of the offensive capabilities of its drone swarms by the DRDO as "impressive."[38] The DRDO released a statement noting that its Young Scientist Laboratory for Asymmetric Technologies is engaged in the development of swarm technologies.[39]

The Indian Army is currently working to acquire capabilities in areas like AI, autonomous weapons systems, quantum technologies, robotics, cloud computing, and algorithmic warfare and has reportedly started teaming up with start-ups; micro, small, and medium-sized enterprises; and others in the private sector, academia, the DRDO, and Defence Public Sector Undertakings. One of the projects undertaken is AI offensive drone operations, which involves an Indian start-up company.[40] In January 2021, the Indian Army engaged in an offensive use of drone technology during an army parade.[41] The drone swarm used at the parade was developed by the army in partnership with a Bengaluru-based start-up, New Space Research and Technologies.[42] These drones, capable of flying up to 40 kilometers into an adversary's territory, can engage in automated, randomized sonic missions on the target by utilizing AI and onboard adaptive computers that are fed with regular satellite feeds, which enable better targeting options. Nevertheless, Indian capabilities in the area of autonomous weapons are fairly limited.

Given the Chinese efforts at converting older tanks into large fleets of unmanned battle tanks, where the future ones will be equipped with AI, the Indian establishment is planning to procure tanks that are smart in terms of their ability to incorporate AI-enabled applications. The Indian Army plans to induct these new tanks by 2030.[43]

Similarly, Chinese development of AI underwater systems has made the Indian establishment and policy community think hard about the capabilities required to address maritime security concerns in the Indian Ocean.[44] The Indian Navy has highlighted its key technological gaps, including sonar equipment, helicopters, and torpedoes. For instance, it made a pitch for "mini drones equipped with passive sonar devices," and senior navy officials have reportedly sought "high endurance autonomous underwater vehicles" for antisubmarine and reconnaissance missions.[45] Despite the push by the Indian Navy, there does not appear to be much progress on the procurement front. In October 2021, the Indian government reportedly made a decision to

---

37 "With Eye on Future, DRDO Aims for AI, Robotics," *Times of India*, April 14, 2018, https://timesofindia.indiatimes.com/city/chennai/with-eye-on-future-drdo-aims-for-ai-robotics/articleshow/63753707.cms.

38 Bhargav and Aveek Sen, "AI Powered Drone New Tool of Warfare," *Pioneer*, November 28, 2021, https://www.dailypioneer.com/2021/sunday-edition/ai-powered-drone-new-tool-of-warfare.html.

39 Rahul Singh, "DRDO Displays Drone Swarm in Offensive Role," *Hindustan Times*, November 18, 2021, https://www.hindustantimes.com/india-news/drdo-displays-drone-swarm-in-offensive-role-101637150019067.html.

40 Rajat Pandit, "Army Showcased Intent to Use 'Drone Swarms' in Offensive Operations in Future," *Times of India*, January 16, 2021, https://timesofindia.indiatimes.com/india/army-showcased-intent-to-use-drone-swarms-in-offensive-operations-in-future/articleshow/80291209.cms.

41 "Indian Army Demonstrates Drone Swarms During Army Day Parade," Ministry of Defence (India), Press Release, January 15, 2021, https://pib.gov.in/PressReleasePage.aspx?PRID=1688807.

42 Singh, "DRDO Displays Drone Swarm."

43 "Indian Army Targets Artificial Intelligence-Powered Battle Tanks with Eye on China," Indian Defence News, June 5, 2021, http://www.indiandefensenews.in/2021/06/indian-army-targets-artificial.html.

44 Naresh Chand, "Unmanned/Autonomous Underwater Vehicles," *SP's Naval Forces*, March 2014, https://www.spsnavalforces.com/story/?id=328.

45 Singh, "How India, Too, Is on a Quest"; and "Request for Information (RFI) for Procurement of High Endurance Autonomous Underwater Vehicles," Ministry of Defence (India), May 14, 2018, https://www.indiannavy.nic.in/sites/default/files/tender_document/RFI%20FOR%20HEAUV-001.pdf?download=1.

procure unmanned aerial and underwater platforms to augment its surveillance capabilities in the Indian Ocean region, but the naval officials who spoke to the media also conveyed that these platforms will be mostly developed indigenously.[46] Meanwhile, in February 2022, the Indian government put on hold the military's plans to acquire 30 Predator armed drones from the United States for the three services.[47] The decision to halt procurement of the drones was reportedly taken for two reasons: to give momentum to the "Make in India" initiative and due to the high cost of the Predator drones.

India's plans for acquiring capabilities face a number of obstacles. The first is budgetary. India's military budget is heavily focused on pay and pensions instead of capital expenditure, which raises questions about whether there will be funds for expensive high-technology weapons. Another serious obstacle is that India is increasingly focused on domestic military R&D, and its previous efforts in this direction do not give much cause for optimism. Whether India now has the capability to develop such systems remains to be seen. An additional limitation is the ongoing confrontation on its border with China. The territorial dispute diverts a lot of resources, both because it is troop-intensive and because India is undertaking significant modernization of its military to deal with the threat.

Partnering with the United States

In response to shared threat perceptions about China, India and the United States have stepped up their partnership in a number of critical and emerging technology areas, including space and cybersecurity. This partnership benefits both powers. For India, there are at least three benefits. The first is that India is able to avail itself of the United States' vastly superior intelligence capabilities, especially with respect to the disposition of forces and capabilities in China's western theater. There are indications that the United States has already helped India with such intelligence during the confrontations in both Galwan and Doklam.[48] Of course, U.S. intelligence capabilities are even more vast and superior when it comes to overall Chinese political, diplomatic, and military activities, which could be of great benefit to India.

Second, there are several niche areas where U.S. technology could augment Indian military capabilities. India has already improved its maritime surveillance capability with the U.S.-built P-8I aircraft and its ground capability with AH-64 Apache helicopter gunships, among other capabilities. Going forward, such niche capabilities would greatly enhance other areas of Indian military power.

Third, India already faces a two-front challenge on its western and northern borders. As the PLA Navy expands, India is likely to face a three-front challenge. Its military budget is already strained and is unlikely to be able to match China's naval advances. U.S. maritime capabilities

---

[46] Hanan Zaffar, "Indian Navy to Acquire Unmanned Aerial and Underwater Systems," Defense Post, November 23, 2021, https://www.thedefensepost.com/2021/11/23/indian-navy-unmanned-systems.

[47] Shishir Gupta, "Plan to Buy Predator Drones Put on Hold," *Hindustan Times*, February 23, 2022, https://www.hindustantimes.com/india-news/plan-to-buy-predator-drones-put-on-hold-101645565612604.html.

[48] "India-China Tensions: Allies Help India Muscle Up for a Hostile Neighbourhood," *Economic Times*, June 29, 2020, https://economictimes.indiatimes.com/news/defence/india-china-tensions-allies-help-india-muscle-up-for-a-hostile-neighbourhood/getting-battle-ready/slideshow/76684625.cms; Suhasini Haidar, "U.S., India Have 'Close Cooperation' on LAC Action by China: Kenneth Juster," *Hindu*, January 5, 2021, https://www.thehindu.com/news/national/us-india-have-close-cooperation-on-lac-action-by-china-kenneth-juster/article33503654.ece; and Pranab Dhal Samanta, "U.S.' Comcasa Assurance: Won't Share India Data without Consent," *Economic Times*, September 5, 2018, https://economictimes.indiatimes.com/news/politics-and-nation/us-comcasa-assurance-wont-share-india-data-without-consent/articleshow/65678934.cms.

would help reduce this burden. Given India's limited resources, having friendly naval forces to supplement its capabilities would be of great assistance. At the current moment, though India conducts naval exercises with a number of countries, the only one that can supplement Indian capabilities with its own forces is the United States, which has a considerable naval presence in the region. For instance, future collaboration could involve joint or coordinated monitoring of Indo-Pacific maritime spaces.

For the United States, a more capable Indian military would help tie down substantial portions of China's ground and air power in Tibet, preventing the PLA from focusing on other theaters. Though India's maritime capabilities are limited, it is still possible for the country to engage in burden-sharing and coordination with the United States and its allies' naval forces, thus helping everybody.

One important area of cooperation concerns a bilateral supply chain resilience pact. Supply chain security and resilience are key for security in the space and cyber domains, as well as the security of autonomous weapons. This is important for securing raw materials and other resources but also significant for ensuring steady supplies and minimizing material supply interruptions. India is already engaged in a trilateral supply chain resilience initiative with Australia and Japan, which should be expanded to include the United States. This could include establishing dedicated industrial parks, improving connectivity in maritime and air corridors, and creating better incentives and an investment-friendly atmosphere to strengthen the initiative.

India and the United States should also strengthen cooperation in such areas as outer space, cyberspace, AI, and automation. This could be taken up under platforms like the Indo-U.S. Science and Technology Forum, which was established through an agreement signed in March 2000. Another viable platform is the bilateral Defence Policy Group, a senior-level official forum between the Indian Ministry of Defence and the U.S. Department of Defense. India and the United States could pursue such cooperation through the India-U.S. Defense Technology and Trade Initiative as well. Given the senior-level attention and oversight under the initiative, delays and barriers caused by bureaucratic processes and legal requirements are dealt with in a more timely fashion. Deepening industry-to-industry collaboration between the two countries on space, cyber, AI, and automation could be mutually beneficial as well. The focus here should not be on the big industries alone but on creating a value chain across start-ups as well as small and medium-sized enterprises at multiple levels for strengthened cooperation on these key technologies.

India is also expanding its partnerships with other countries in the areas of these critical and emerging technologies. On cybersecurity, CERT-In has concluded agreements with Japan, Malaysia, and Singapore, with the discussions focused on issues such as cybersecurity incident trends, updated information on the latest threats, and best practices to augment cybersecurity.[49]

Conclusion

China's technological advancements in the areas of outer space, cyberspace, and autonomous weapons are likely to strongly affect the security of India and other Indo-Pacific powers. China's pursuit of these capabilities could be U.S.-centric, but the national security implications for India are consequential, exacerbating the vulnerabilities that it already faces vis-à-vis China. India

[49] Ministry of Electronics and Information Technology (India), "Lok Sabha Unstarred Question No. 573: Cyber Security," November 20, 2019, http://164.100.24.220/loksabhaquestions/annex/172/AU573.pdf.

cannot respond to China's accelerated capability developments and aggressive behavior on its own. Partnership with the United States and other like-minded countries will be a significant aspect of India's efforts to manage the strategic consequences of China's rise, including within the technologies explored in this essay.

India and the United States already have several new initiatives to further their collaboration in the emerging and critical technology sector. The U.S.-India Initiative on Critical and Emerging Technologies, technology partnerships within the Quad both for collaborating on technology and for writing the global rules of the road for regulating these technologies, and a partnership on resilient supply chains are important pieces of the deepening engagements between New Delhi and Washington. But there are more opportunities for collaboration. On outer space, for instance, the two countries could collaborate on creating better space situational awareness, which is critical given their growing dependencies on space as well as the vulnerabilities in this domain. Similarly, on cyberspace, there could be greater coordination on framing global governance measures guided by the multistakeholder approach that brings together all the different stakeholders who have an interest in how cyberspace is governed. Finally, India is party to minilaterals focused on supply chain resilience involving Australia and Japan. This would be an ideal area for U.S. participation, making existing efforts a Quad initiative.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

New Domains of Chinese Military Modernization: Security Implications for Japan

Yuka Koshino

YUKA KOSHINO is a Research Fellow for Security and Technology Policy at the International Institute for Strategic Studies (IISS). She can be reached at <yuka.koshino@iiss.org> or on Twitter <@YukaKoshino>.

EXECUTIVE SUMMARY

This essay examines Japan's perceptions of and responses to major threats posed by China's emerging capabilities in space, cyber, and autonomous weapons systems and considers policy options for further cooperation with the U.S. and its regional partners and allies to counter these threats.

MAIN ARGUMENT

Momentum is growing for Japan to enhance its defense capabilities and update its security policies amid heightened security concerns over China's military modernization. Japanese leaders have become increasingly concerned about China's military-civil fusion strategy to adopt innovative technologies to accelerate its development of a world-class military by 2049. This strategy would allow China to asymmetrically challenge the United States and its regional allies, including Japan. Such a challenge could threaten Japanese security through increased Chinese aggression in the East China Sea or Taiwan Strait. The risk of a contingency on any of these fronts has also increased concern among the Japanese public and stressed the need for updated security and defense strategies. As a result, there is heightened public support for Japan to assume greater regional and global security roles and responsibilities. Updates to improve the effective deterrence and response capabilities of both Japan and the U.S.-Japan alliance would entail improving coordination within the Japan Self-Defense Forces, adopting a more active defense posture, increasing defense spending, and making investments in R&D for future warfighting in the domains of space, cyber, and autonomous weapons systems.

POLICY IMPLICATIONS

- Enhanced bilateral coordination between the U.S. and Japan would improve preparedness for a potential contingency in the Taiwan Strait and enhance Japan's counterstrike capabilities, should Japan change its policy to adopt the capabilities.
- Involving Japan in U.S. ally–led initiatives to cultivate joint capabilities, such as the AUKUS partnership between Australia, the United Kingdom, and the U.S., would accelerate the country's development and military adoption of emerging and disruptive technologies.
- Leveraging commercial industrial partnerships between the U.S. and Japan, especially in the realm of advanced communications technologies, would help achieve multidomain integration and allow for enhanced defense.

In recent years, Japanese policymakers, security thought leaders, and the public have become increasingly concerned about the rise in Chinese military spending and China's effort to rapidly adopt emerging technologies to modernize its forces to challenge the U.S. military's presence and capabilities in the Indo-Pacific region. Under President Xi Jinping, the People's Republic of China (PRC) is pursuing ambitious goals to develop a world-class military by 2049, with a focus on technologies in new domains such as space and cyber. In 2015 the country designated space and cyber as critical for warfighting and announced that it seeks to achieve superiority in those domains.[1] In July 2017, the PRC also announced that it aims to become a world leader in artificial intelligence (AI).[2] At the 19th Party Congress of the Chinese Communist Party (CCP), Xi further guided the People's Liberation Army (PLA) to adopt AI by urging the need to "accelerate intelligentization, and improve joint operations capabilities and all-domain combat capabilities based on network information systems."[3] China has been pursuing a military-civil fusion strategy to adopt innovative technologies developed in commercial spaces to accelerate the PLA's effort.[4]

While many unknowns remain regarding the PLA's ability to adopt emerging technologies in these domains and for its operations, growing capabilities in space and cyber, and potential improvements in the automaticity of weapons systems, could allow China to meet its military modernization goals and asymmetrically challenge the deterrence created by the United States and its regional allies, including Japan.[5] Moreover, the U.S. Department of Defense assessed in 2021 that the "PLA's evolving capabilities and concepts continue to strengthen the PRC's ability to 'fight and win wars' against a 'strong enemy,' coerce Taiwan and rival claimants in territorial disputes, counter an intervention by a third party in a conflict along the PRC's periphery, and project power globally."[6] This observation implies that the United States' ability to coordinate with Japan in a case of Chinese aggression near Japanese territory, in the East China Sea, or in the Taiwan Strait could be challenged and poses a serious threat to Japanese security.

Since a high-level U.S. military official stated in March 2021 that China could invade Taiwan by 2027, concerns have risen in Tokyo about the implications of a Taiwan contingency for Japan's defense and its role in such a situation.[7] Following China's assertive military exercises in the East China Sea in August 2022, in which five ballistic missiles dropped into Japan's exclusive economic zone for the first time, concerns in the Japanese public have also increased.[8] The Russian war against Ukraine and the role of new domains and capabilities such as cyber, unmanned aerial vehicles (UAVs), and space technologies have further catalyzed the debate in Tokyo about adopting

---

1 State Council Information Office of the People's Republic of China (PRC), *China's Military Strategy* (Beijing, May 2015), http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

2 "China Issues Guideline on Artificial Intelligence Development," State Council Information Office (PRC), Press Release, July 20, 2017, http://english.www.gov.cn/policies/latest_releases/2017/07/20/content_281475742458322.htm.

3 Elsa B. Kania, "Global China: 'AI Weapons' in China's Military Innovation," Brookings Institution, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.

4 See, for example, Meia Nouwens and Helena Legarda, "China's Pursuit of Advanced Dual-Use Technologies," International Institute for Strategic Studies (IISS), December 18, 2018, https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance.

5 For Chinese military modernization goals, see, for example, Brian Hart, Bonnie S. Glaser, and Matthew P. Funaiole, "China's 2017 Goal Marks the PLA's Centennial, Not an Expedited Military Modernization," Jamestown Foundation, China Brief, March 26, 2021, https://jamestown.org/program/chinas-2027-goal-marks-the-plas-centennial-not-an-expedited-military-modernization.

6 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2021* (Washington, D.C., November 2021), v, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

7 Helen Davidson, "China Could Invade Taiwan in Next Six Years, Top U.S. Admiral Warns," *Guardian*, March 10, 2021, https://www.theguardian.com/world/2021/mar/10/china-could-invade-taiwan-in-next-six-years-top-us-admiral-warns.

8 Ryo Nemoto and Reiko Miki, "5 Chinese Missiles Land in Japan's EEZ: Defense Chief," *Nikkei Asia*, August 4, 2022, https://asia.nikkei.com/Politics/International-relations/US-China-tensions/5-Chinese-missiles-land-in-Japan-s-EEZ-defense-chief.

a more active defense posture and drastically increasing defense spending to reach NATO countries' spending levels (2% of GDP in the next five years) and to study and invest in capabilities required for future warfighting in the new domains.[9]

Against this backdrop, this essay examines Japan's perceptions of and responses to major threats posed by China's growing capabilities in space, cyber, and autonomous weapons systems. It then considers policy options for further cooperation between the United States and its regional partners and allies to counter these threats.

Threats from China's Space, Cyber, and Autonomous Capabilities

Citing Chinese military strategies and authoritative analyses, Japanese analysts observe that space, cyber, and autonomous technologies are essential for the PLA to achieve its goal of developing "informationized [cyber-enabled]" and "intelligentized" or "autonomous" armed forces in the future.[10] Rapid development of these capabilities has the potential to challenge Japanese security in the following four ways in the short, medium, and long term in peacetime, a gray-zone situation, and a potential contingency scenario.

First, the PLA's kinetic and nonkinetic anti-satellite (ASAT) capabilities and cyber offensive capabilities are an immediate concern for Tokyo because they could asymmetrically disrupt and neutralize the Japan Self-Defense Forces (JSDF) and U.S. military in a gray-zone situation or a potential contingency. In the kinetic realm, China demonstrated the first successful testing of its ASAT capabilities in 2007. Further, the U.S. Department of Defense and a research institute suggest, after analyzing China's May 2013 space launch, that Beijing may have developed an ASAT weapon that could reach out to geostationary orbit, an altitude of more than 35,000 kilometers.[11] Such a system poses a direct threat to the JSDF's X-band satellites and the Quasi-Zenith Satellite System—Japan's satellite navigation constellation backup for the U.S. Global Positioning System (GPS)—which are located at this altitude.

Nonkinetic counterspace capabilities, such as lasers, navigation signal-jamming, and spoofing, are also gaining Tokyo's attention as capabilities that could disrupt regional military communications. The 2018 revision of Japan's National Defense Program Guidelines (NDPG), for instance, highlighted these capabilities as challenges in the electromagnetic spectrum. A 2019 Cabinet Office assessment also highlighted China's establishment of vehicle-mounted long-range jammers on Fiery Cross Reef and the Spratly Islands in the South China Sea as potential threats to military communications systems in the region.[12] The potential misuse of these capabilities against Japanese and regional assets could trigger an unexpected escalation from a gray-zone competition

---

[9] See, for example, Liberal Democratic Party (LDP) Security Research Council, "Aratana kokka anzenhosho senryaku nado no sakutei ni muketa teigen" [A Proposal for a New National Security Strategy Development], April 26, 2022, 2, https://jimin.jp-east-2.storage.api.nifcloud.com/pdf/news/policy/203401_1.pdf.

[10] For Japanese views on Chinese military modernization in the space and cyber domains and Chinese military strategies, see Yuka Koshino, "China's Military Modernization in Space and Cyber and the Implications for the U.S.-Japan Alliance," in "Meeting China's Military Challenge: Collective Responses of U.S. Allies and Security Partners," ed. Bates Gill, National Bureau of Asian Research, NBR Special Report, no. 96, January 2022, https://www.nbr.org/publication/chinas-military-modernization-in-space-and-cyber-and-the-implications-for-the-u-s-japan-alliance.

[11] See, for instance, Marc V. Schanz, "Report Claims China Space Launch Was ASAT Weapon Test," *Air Force Magazine*, March 24, 2014, https://www.airforcemag.com/report-claims-china-space-launch-was-asat-weapon-test; and U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2021*, 37, https://dod.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf.

[12] Cabinet Office of Japan, "Uchu o meguru josei henka: Uchu anzen hosho no jyuyosei notakamari" [Changes in Space Environment: Growing Importance of Space Security], October 3, 2019, https://www8.cao.go.jp/space/comittee/27-anpo/anpo-dai33/siryou3-2-2.pdf.

to a potential conflict, especially in the highly contested maritime space in the East and South China Seas.

In the cyber domain, recent research suggests that China is developing offensive capabilities to deploy in peacetime and the early phases of conflict. The country focuses on technologies to conduct both reconnaissance and attacks by penetrating the adversary's network during peacetime. The PLA is further exploring advanced capabilities of "integrated network electronic warfare," which "would enable it to insert malicious algorithms into adversary networks even if a wire connection does not exist."[13] Tokyo recognizes China's growing offensive capability and potential for using hybrid warfare to attack remote islands in the East China Sea. Japanese policymakers have referred to the role of cyber capabilities in the early phases of Russia's invasions of Ukraine in 2014 and 2022 and suggested that the PLA could use similar tactics in an invasion of Taiwan.[14] The Russian attack against Ukrainian nuclear power plants also raised concerns about a potential Chinese cyberattack against Japanese critical infrastructure as a means to keep Japan from supporting the U.S. military in a contingency situation with Taiwan. The ability of China to plausibly deny the attack and challenge Japan's defense capabilities further adds to Tokyo's concerns.[15]

Second, the PLA's rapid investment in space and autonomous technologies poses mid- to long-term threats to existing missile and nuclear deterrence by enhancing the accuracy and decision-making speed of China's operations. In the short to medium term, rapid investment and enhancements in China's space capabilities, such as space situational awareness (SSA), intelligence gathering, and space-based communication and navigation capabilities, could allow the PLA Rocket Force to improve the operational capabilities of its missiles in terms of decision-making speed and accuracy, as well as improve its anti-access/area-denial capabilities. Furthermore, according to Elsa Kania, the PLA Rocket Force may leverage AI-driven remote sensing, targeting, and decision support for its missile launches, and its missiles may incorporate a greater degree of automation to facilitate operations.[16] The implications of these efforts by the PLA Rocket Force for China's new missile capabilities, including hypersonic glide vehicles and cruise missiles, are even more concerning for Tokyo and Washington after China's successful testing of the Fractional Orbital Bombardment System for its nuclear-capable hypersonic orbital glide vehicle in October 2021.[17] China thus has the potential to obtain a prompt global strike nuclear capability and challenge the strategic deterrence created by the United States.[18]

These developments raise several concerns for Tokyo. The first is the challenge posed to Japan's ability to defend its remote Senkaku and Nansei Islands in the East China Sea. A second concern is whether the United States would commit to defending the Senkaku Islands and to providing extended nuclear deterrence.[19] Moreover, Tokyo is worried about the PLA's ability to deter and

---

[13] IISS, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 97–98, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[14] See, for example, LDP Security Research Council, "Aratana kokka anzenhosho senryaku nado no sakutei ni muketa teigen."

[15] Jun Murai, "Why Cyber Defense in Japan Is So Unreliable," *Japan Times*, January 17, 2022, https://www.japantimes.co.jp/opinion/2022/01/17/commentary/japan-commentary/japan-cyber-security.

[16] Kania, "Global China: 'AI Weapons,'" 3.

[17] Timothy Wright, "Is China Gliding Towards a FOBS Capability?" IISS, October 22, 2021, https://www.iiss.org/blogs/analysis/2021/10/is-china-gliding-toward-a-fobs-capability.

[18] Sandra Erwin, "China's Hypersonic Vehicle Test a 'Significant Demonstration' of Space Technology," *SpaceNews*, October 22, 2021, https://spacenews.com/chinas-hypersonic-vehicle-test-a-significant-demonstration-of-space-technology.

[19] Greg Austin, Timothy Wright, and Rajeswari P. Rajagopalan, "Military Ambitions and Competition in Space: The Role of Alliances," IISS, February 7, 2022, https://www.iiss.org/blogs/research-paper/2022/02/military-ambitions-and-competition-in-space-the-role-of-alliances.

counter U.S. or Japanese intervention in and around the Taiwan Strait. According to the U.S. Department of Defense, these capabilities include "direct ascent, co-orbital, electronic warfare, and direct energy capabilities."[20] By other accounts, the PLA Navy is also experimenting with unmanned surface vessels and submarines with limited autonomy to gain competitiveness in undersea warfare.[21] Despite the sophistication of these emerging technologies, however, experts on the PLA suggest that its ability to operationalize autonomous technologies is uncertain and will depend on other factors, such as the ability to overcome organizational challenges in testing, training, and conceptualization.[22]

Third, cyber-enabled espionage by PLA-related hacking groups against Japanese civilian and defense-related research institutes, companies, and government agencies also threatens the JSDF's technological advantage over the PLA. The civilian sector is leading innovation in AI, space, robotics, big data, and quantum technologies, with which China seeks to develop a more efficient and modern joint force. China has a track record of using cyber-enabled information theft, and Japanese private-sector companies and research institutes have reported cases of industrial espionage, despite their emphasis on protecting their advanced technological base from Chinese operations.[23]

According to Japanese government sources, there have been more than ten reported cases of cyberattacks against defense-related Japanese industries and organizations that resulted in a breach of personal, technological, and business information, with at least two cases being widely recognized as attacks from China.[24] While Tokyo has historically hesitated to attribute attacks to a specific country, China was widely reported as responsible for the June 2019 attack against Mitsubishi Electric Company's network, which is said to have breached information relevant to the Japanese Ministry of Defense's hyper-velocity projectile R&D project.[25] Moreover, in April 2021 the Japanese Metropolitan Police for the first time recognized a member of the CCP as connected to a PLA-backed hacking group responsible for a large cyberattack against Japanese research institutes and civilian, commercial, and defense firms working in space industries.[26] Space and hypersonics are focus areas for Japan's efforts to enhance its missile defense systems, and losing technological advantage in these areas could pose serious challenges to Japan's future deterrence capabilities discussed above.

Last, fundamental ethical and reliability questions remain about China's efforts to add automaticity to capabilities that have the potential for escalation in a phase of military engagement. The Ministry of Science and Technology's ethical guidelines for AI, published in October 2021, offered assurances that China likely shares human-centric approaches to AI. The guidelines emphasize that "humans have fully autonomous decision-making rights and that they have the right to accept or reject AI-provided services" to assure the "controllability and trustworthiness"

---

20 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2021*, vii.

21 Kania, "Global China: 'AI Weapons,'" 3.

22 Ibid., 7.

23 Jeff Jones, "Confronting China's Efforts to Steal Defense Information," Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2020, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

24 This information is from a document obtained by the author from Japan's Acquisition, Technology and Logistics Agency in May 2022.

25 Kaigo Narisawa, "Cyberattack at Mitsubishi Electric a Security Threat," *Asahi Shimbun*, December 25, 2021, https://www.asahi.com/ajw/articles/14510480.

26 "Chinese Military Seen Behind Japan Cyberattacks," *Japan Times*, April 20, 2021, https://www.japantimes.co.jp/news/2021/04/20/national/chinese-military-japan-cyberattacks.

of systems.[27] Yet one might question the reliability and safety of such systems. For instance, Kania suggests that the "Chinese military could rush to deploy weapons systems that are unsafe, untested, or unreliable under actual operational conditions."[28] Given the rising tensions in the air and maritime areas near Japan's remote islands and in the Taiwan Strait, the possibility of these autonomous systems, with their greater decision-making speed, unintentionally escalating a military engagement into a conflict cannot be discounted. Moreover, questions remain about the quality of data collected by the PLA, which does not have combat experience. Inaccurate data has the potential to further undermine the reliability of these systems.

Japan's Responses and Challenges

Responses

Over the past decade, since the second Shinzo Abe government formed in 2012, Tokyo has taken several significant steps to enhance its security posture both internally and externally with the United States in order to pursue a more active role in dealing with the deteriorating security environment. Efforts such as the establishment of the National Security Council and its administrative body in December 2013, the cabinet decision to allow limited exercise of collective self-defense in July 2014, the upgrade of the U.S.-Japan Defense Guidelines in 2015, and the passage of security-related bills in the same year were significant in achieving closer policy coordination and defense cooperation with the United States and other like-minded security partners.[29] To counter the above challenges arising from the PLA's space, cyber, and autonomous technology capabilities, Tokyo has responded in the following five ways.

First, Japan has improved the jointness of its forces by integrating capabilities across multiple domains, including space and cyber. The most notable change in its defense policy is the introduction of a new defense concept to build a "multi-domain defense force" under the revised NDPG and Medium-Term Defense Plan (MTDP) in 2018.[30] While the primary goal is to realize cross-domain operations rather than the U.S. forces' multidomain operational concept, the JSDF has enhanced jointness across domains, including in space and the electromagnetic spectrum.[31] The 2018 NDPG was also significant because it recognized the priority to "achieve superiority in space and cyber domains" against its competitors' growing capabilities. Tokyo further officially called out Chinese, along with North Korean and Russian, cyber capabilities, including military cyber capabilities, in the 2021 Cybersecurity Strategy and acknowledged the threat arising from these capabilities.[32]

As part of these efforts to improve the effectiveness and efficiency of operations in space and cyber, the Ministry of Defense has conducted a major restructuring of units to achieve greater jointness across branches. It announced plans for a Space Operations Group to establish a new

---

27 "Ethical Norms for New Generation Artificial Intelligence Released (Translation)," Center for Security and Emerging Technology, October 21, 2021, https://cset.georgetown.edu/publication/ethical-norms-for-new-generation-artificial-intelligence-released.

28 Kania, "Global China: 'AI Weapons,'" 1.

29 See Koshino, "China's Military Modernization in Space and Cyber."

30 Ministry of Defense (Japan), "National Defense Program Guidelines (NDPG) and Medium Term Defense Program (MTDP)," https://www.mod.go.jp/en/d_policy/basis/guideline/index.html.

31 Ibid.

32 Government of Japan, "Cybersecurity Strategy," September 28, 2021, 9, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en.pdf.

command-and-control unit in the space domain.[33] In the realm of cyber, it established the tentatively named Japan Self-Defense Force Cyber Defense Command in March 2021 to integrate the various units tasked with defending the Ministry of Defense and JSDF networks, such as the Cyber Defense Group established in 2014 and cyber-related units deployed in the ground, maritime, and air forces.[34] The ministry is also investing to improve the survivability of the JSDF's command and communications (C2) systems and networks.[35] It commissioned research in 2021 to closely study Japan's future warfighting strategies vis-à-vis China and the capabilities required to develop a multidomain force with input from the United States.[36]

Second, Japan has accelerated its investments in defensive capabilities to monitor, gather intelligence on, and respond to Chinese activities in the space and cyber domains. In space, it established a space operations squadron in 2020 to enhance monitoring capabilities. The unit will operate ground-based and space-based SSA capabilities, which will be developed by mid-2023.[37] Japan's efforts in space also aim to enhance defense cooperation under the U.S.-Japan alliance. For instance, the space operations squadron is expected to share information gathered through SSA with U.S. Space Command.[38] Further, Japan agreed in 2019 to host U.S. sensors in Japan's Quasi-Zenith Satellite System, also to be launched in 2023.[39] In 2021 the Ministry of Defense announced plans to establish a second space squadron to "detect jamming against Japan's satellites."[40] Tokyo has also begun cooperating with the United States and its allies in tabletop exercises for SSA and wargames—taking part in U.S. Strategic Command's Global Sentinel since 2016 and in the Schriever Wargame since 2018.[41]

In the cyber domain, the Ministry of Defense expanded the scope of the Cyber Defense Group, which was established in 2014 to monitor and respond to cyberattacks.[42] To respond effectively to cyberattacks, Japan is also developing "active defense" capabilities—offensive capabilities to disrupt an opponent's use of cyberspace in the case of an attack against Japan.[43] According to budget documents, the Japanese government is exploring new AI-enabled responses to attacks

---

33 Ministry of Defense (Japan), "Defense Programs and Budget of Japan: Overview of FY 2021 Budget," 5, https://www.mod.go.jp/en/d_act/d_budget/pdf/210331a.pdf.

34 Ministry of Defense (Japan), "Defense Programs and Budget of Japan: Overview of FY 2021 Budget," 6; and "Japan's SDF Launches New Cyber-Defense Unit," Kyodo News, March 17, 2022, https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html.

35 Ministry of Defense (Japan), *Defense of Japan 2021* (Tokyo, July 2021), 216, https://www.mod.go.jp/en/publ/w_paper/wp2021/DOJ2021_EN_Full.pdf.

36 See Jeffrey Hornung et al., "Preparing Japan's Multi-Domain Defense Force for the Future Battlespace Using Emerging Technologies," RAND Corporation, July 2021, https://www.rand.org/pubs/perspectives/PEA1157-1.html.

37 For details on the space domain mission unit, see Yuka Koshino, "Japan's New Space Domain Mission Unit and Security in the Indo-Pacific Region," IISS, May 1, 2020, https://www.iiss.org/blogs/military-balance/2020/05/japan-space-domain-mission-unit-security.

38 "Launch of the Space Operations Squadron," Ministry of Defense (Japan), Japan Defense Focus, https://www.mod.go.jp/en/jdf/no125/specialfeature.html#article01; and "Japan Air Self Defense Force to Present SSA Updates at Military Space Situational Awareness 2021," Space Data Association, April 2021, https://www.space-data.org/sda/news/japan-air-self-defense-force-to-present-ssa-updates-at-military-space-situational-awareness-2021.

39 "U.S.-Japan Security Consultative Committee 2019," U.S. Department of State, Fact Sheet, April 19, 2019, https://2017-2021.state.gov/u-s-japan-security-consultative-committee-2019-fact-sheet/index.html.

40 "Japan to Launch Second Outer Space Operations Unit in Fiscal 2022," *Nikkei Asia*, November 14, 2021, https://asia.nikkei.com/Politics/Japan-to-launch-second-outer-space-operations-unit-in-fiscal-2022; and Ministry of Defense (Japan), "Defense Programs and Budget of Japan: Overview of FY 2022 Budget Request," 5, https://www.mod.go.jp/en/d_act/d_budget/pdf/220330a.pdf.

41 Hidetaka Yoshimatsu, "Japan's International Engagements in Outer Space," Australian Institute of International Affairs, June 15, 2021, https://www.internationalaffairs.org.au/australianoutlook/japans-international-engagements-in-outer-space.

42 Franz-Stefan Gady and Yuka Koshino, "Japan and Cyber Capabilities: How Much Is Enough?" IISS, August 28, 2020, https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities.

43 Ministry of Defense (Japan), "National Defense Program Guidelines for FY 2019 and Beyond," December 18, 2018, 20, https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf.

against its systems and new technologies to enhance resilience against cyberattacks against JSDF equipment.[44] These cyberdefense capabilities are essential for the security of space systems on the ground, which would likely become the targets of cyberattacks from China. Tokyo also has enhanced cyberdefense cooperation with the United States and its allies by taking part in NATO-led exercises and holding cyber dialogues with several like-minded countries, including Australia, the United Kingdom, Germany, and Estonia.[45]

Third, Japan has stepped up its effort to enhance its missile deterrence capabilities—from deterrence by denial to deterrence by punishment, or from the possession of purely defensive to limited offensive capability—as China, North Korea, and Russia rapidly progress in their missile development. To enhance ballistic missile defense against new missile technologies, such as hypersonic glide vehicles, Japan is developing an early-warning satellite constellation with the United States to deploy in the mid-2020s.[46] To enhance the defense of its remote islands, Japan is further seeking to acquire and develop standoff missile capabilities. The 2018 NDPG and MTDP stated goals for procurement and R&D in standoff defense capabilities, and the JSDF has since launched four R&D programs to develop indigenous capabilities. Efforts include the improvement of Type 12 surface-to-ship guided missile capabilities, anti-ship missiles, hypervelocity gliding projectiles, and hypersonic cruise missiles.[47]

These standoff missiles will likely be used for counterstrike capability, which Prime Minister Kishida Fumio's administration has expressed interest in obtaining by the end of 2022.[48] The adoption of such a capability would be a major policy shift by Tokyo. It not only would give Japan an offensive capability but could alter the historical division of labor under the U.S.-Japan alliance, where Japan has served as the "shield" and the United States as the "spear." According to the April 2022 proposal by the Liberal Democratic Party (LDP), counterstrike capabilities should target the enemy's C2 infrastructure in addition to its bases.[49] The proposal also stated the need to develop related capabilities, such as the use of UAVs to enhance intelligence, surveillance, and reconnaissance (ISR); active defense capabilities in the space, cyber, and electromagnetic spectrums; and nonkinetic capabilities, such as the deployment of decoys.[50] Tokyo is further considering the deployment of electromagnetic railguns by the late 2020s as a core capability to intercept Chinese hypersonic weapons systems. In 2022, it earmarked R&D funding to develop basic technology and prototyping of the railguns.[51]

Fourth, Japan has expanded its near- to long-term R&D programs in order to enhance deterrence and effectively respond to the PLA's use of advanced weapons systems, particularly in the realm of autonomous technologies. One such development is autonomous collaborative

---

44 Ministry of Defense (Japan), "Defense Programs and Budget of Japan: Overview of FY 2021 Budget," 6.

45 Ministry of Defense (Japan), *Defense of Japan 2021*, 285.

46 See, for example, "Japan to Mull Joining U.S. 'Satellite Constellation' Initiative to Counter Missile Threats," *Mainichi*, January 12, 2021, https://mainichi.jp/english/articles/20210112/p2a/00m/0na/012000c; and "(Dokuji) Kogata eiseimo, nijunendai nakaba ni sanki uchiage: Churo no gokuchoonsoku heiki tanchi mo shiya" [(Exclusive) Satellite Constellation to Be Launched in Mid-2020s: Eyeing on Detecting Chinese and Russian Hypersonic Weapons System], *Yomiuri Shimbun*, November 22, 2021, https://www.yomiuri.co.jp/politics/20211121-OYT1T50209.

47 Ministry of Defense (Japan), *Defense of Japan 2021*, 261–63.

48 "Keynote Address by Prime Minister Kishida Fumio at the IISS Shangri-La Dialogue," Prime Minister of Japan and His Cabinet, June 10, 2022, https://japan.kantei.go.jp/101_kishida/statement/202206/_00002.html.

49 LDP Security Research Council, "Aratana kokka anzenhosho senryaku nado no sakutei ni muketa teigen," 10.

50 Ibid., 10.

51 "Japan Set to Develop Railguns to Counter Hypersonic Missiles," *Nikkei Asia*, January 4, 2022, https://asia.nikkei.com/Politics/Japan-set-to-develop-railguns-to-counter-hypersonic-missiles.

unmanned underwater vehicles (UUV) to improve the Japan Maritime Self-Defense Force's underwater warfare capabilities to respond to growing Chinese naval activities around Japan's remote islands.[52] The Acquisition, Technology and Logistics Agency (ATLA) is seeking to develop UUVs that could coordinate with both manned vessels and unmanned systems in the air, ground, and maritime domains to conduct ISR, support missions, and counter activities by the end of the 2030s.[53]

In particular, the Ministry of Defense has focused on enhancing mine countermeasure capabilities to respond to growing PLA Navy submarine activity near the Senkaku Islands. It has invested in UUV technologies for such capabilities since 2008 to enhance the capacity to detect buried mines and has partnered with Mitsubishi Heavy Industries since 2013 to add autonomous technology to its UUVs. The establishment of the Amphibious and Mine Warfare Center in October 2020 and the first-ever deployment of an OZZ-5 autonomous mine countermeasure vehicle on a Maritime Self-Defense Force Mogami-class frigate in 2021 further demonstrate Tokyo's focus on mine countermeasure capabilities. A former JSDF officer suggested that the United States could ask Japan to conduct mine countermeasures in a Taiwan contingency scenario, similar to its request in 1991 after the Gulf War, which resulted in Japan's dispatch of Maritime Self-Defense Force troops to take on the mission in the same year for the first time since 1965.[54]

The Ministry of Defense has also worked to develop and deploy autonomous unmanned combat aerial vehicles (UCAVs) to operate alongside manned future fighter aircraft by the mid-2030s. Its early operational vision suggests that the JSDF would use them in three operational scenarios: (1) counter-air defensive operations, (2) close-air support for the Ground Self-Defense Force in Japanese territory, including on remote islands, and (3) air interdiction to defend Japan's air, sea, and land territories.[55] Its operational concept also suggests that the UCAVs would be capable of detecting adversaries' aircraft and launching air-to-air missiles to enhance control of the air. Given the long timeline for deployment, Tokyo is reportedly seeking to conduct joint training with the U.S. MQ-9 aircraft, which is expected to be deployed in Japan in 2022, to fill the capabilities gap and enhance deterrence against the PLA Navy.[56] The same report also suggested that Japan seeks to jointly develop UCAVs with the United States. While the details of the timeline are unknown, ATLA is also seeking to develop quantum technologies, such as quantum sensing to enhance detection capabilities and quantum communication to enhance cybersecurity for the JSDF's military communications.[57]

Finally, Tokyo has taken a whole-of-government approach to deter cyberattacks and enhance the cybersecurity of civilian agencies and commercial companies operating around national defense. One example is the establishment of the National Center of Incident Readiness and

---

52 Acquisition, Technology and Logistics Agency (ATLA), "R&D Vision: Towards Realization of a Multi-Domain Defense Force and Beyond," Ministry of Defense (Japan), March 31, 2020, 14–15, https://www.mod.go.jp/atla/en/policy/pdf/rd_vision_exp20203_04.pdf.

53 Ibid., 15.

54 Kawakami Yasuhiro, "'Taiwan yuji ni okeru kiraisen (zenpen): Kiraisen no tokucho to kiraisenfusetsusen shinario" [Mine Warfare in Taiwan Contingency (Part 1): Features of Mine Warfare and Its Scenarios], Sasakawa Peace Foundation, December 15, 2021, https://www.spf.org/iina/articles/kawakami_01.html; and Kawakami Yasuhiro, "'Tawan yuji ni okeru kiraisen (kohen): Kiraisen no tokucho to kiraisenfusetsusen shinario" [Mine Warfare in Taiwan Contingency (Part 2): Features of Mine Warfare and Its Scenarios], Sasakawa Peace Foundation, January 7, 2022, https://www.spf.org/iina/articles/kawakami_02.html.

55 Ministry of Defense (Japan), "Reiwa san-nendo seisaku hyoka (jizen no jigyo hyoka)" [Reiwa 3-Year Policy Evaluation Report (Preliminary Project Evaluation)], August 2021, 4, https://www.mod.go.jp/j/approach/hyouka/seisaku/2021/pdf/jizen_08_honbun.pdf.

56 "Japan to Develop Combat Drones to Assist Jet Fighters," *Nikkei Asia*, June 3, 2022, https://asia.nikkei.com/Politics/Japan-to-develop-combat-drones-to-assist-jet-fighters.

57 ATLA, "R&D Vision," 7.

Strategy for Cybersecurity in the Cabinet Secretariat in 2015 to take a cross-government approach to cybersecurity. This included efforts to enhance public-private cooperation to monitor, deter, and respond to cyberattacks through information sharing and tabletop exercises.[58]

Another change is Tokyo's more active stance to attribute responsibility to China for cyberattacks, such as the mention of China in the 2021 Cybersecurity Strategy and the accusation by the Metropolitan Police Agency in April 2021 that a CCP member affiliated with a PLA-backed hacking group was involved in a major hack of Japan's space agency.[59] In May 2022, Tokyo passed and enacted legislation to promote economic security, which includes efforts to reduce cybersecurity risks in basic infrastructure.[60]

Challenges

The growing concerns of a potential contingency in the Taiwan Strait have accelerated public debate in Japan about improving defense capabilities. A May 2022 survey suggested that more than half of the respondents were supportive of a defense spending hike.[61] In fact, the Kishida administration is set to revise the three core security and defense documents—the National Security Strategy, NDPG, and MTDP—and to build on existing responses to deal with a rapidly changing regional and security environment. Reports suggest that Tokyo is seeking to improve Japan's capabilities in the emerging domains of space and cyber, including the AI and autonomous technologies prioritized in the new strategy documents. Yet several fundamental obstacles remain for Tokyo to develop and effectively operationalize these capabilities, both indigenously and through close cooperation with the United States.[62]

From the operational perspective, a set of challenges comes from the current C2 structure of the JSDF. One is the extensive burden on the chief of staff of the Joint Staff Office of the JSDF to oversee operational capabilities in all three branches—ground, maritime, and air—and to lead contingency planning and response. Under the current organizational structure, the joint chief of staff serves both as the combatant commander and as the chief of defense, whose responsibility is to support the civilian defense minister. Former joint chiefs of staff and defense establishments have repeatedly expressed concerns about bandwidth and have proposed the idea of setting up a joint operations command dedicated to enhancing joint operations across the three forces to prepare for a potential contingency.[63] Another challenge is the existing stipulation that limits the JSDF's ability to set up a joint task force capable of conducting cross-domain operations on special occasions such as ballistic missile defense and disaster relief. Under the current guidelines, the

---

58 National Center of Incident Readiness and Strategy for Cybersecurity (Japan), *Cybersecurity Strategy 2021* (Tokyo, September 2021), https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf.

59 "Chinese Military Seen Behind Japan Cyberattacks," *Japan Times*, April 20, 2021, https://www.japantimes.co.jp/news/2021/04/20/national/chinese-military-japan-cyberattacks.

60 Kyosuke Katahira and Tadakatsu Sano, "Japan Enacts Economic Security Law," Jones Day, May 11, 2022, https://www.jonesday.com/en/insights/2022/05/japan-enacts-economic-security-law.

61 Yoshitaka Isobe, "Survey: Record 64% of Japanese Want National Defense Bolstered," *Asahi Shimbun*, May 2, 2022, https://www.asahi.com/ajw/articles/14612368.

62 "Chokyori misairu de shinko yokush boei gaisan yokyu no koshian hanmei" [Deterrence Against Invasion via Long-Range Missiles: Outlines of Budget Request Revealed], *Sankei Shimbun*, August 3, 2022, https://www.sankei.com/article/20220803-I4CJEZH7UVJZRCVB7VS6Y6MLHA.

63 "Josetsu no togo shireibu, Boeisho ga kento, riku kai ku no renkei o enkatsuka" [The MOD Considers Setting Up a Permanent Joint Operations Command to Enhance Collaboration Between Ground, Maritime, and Air Forces], *Nikkei*, October 5, 2013, https://www.nikkei.com/article/DGXNASFS0403T_U3A001C1PP8000; "'Togo shireibu' Josetsu o kento, Jieitai toppu ga genkyu" [JSDF Chief Mentions That He Is Considering Setting Up the Joint Operations Command], *Sankei Shimbun*, March 1, 2016, https://www.sankei.com/article/20160301-ADFFGV5HFZOKROLFZTTVFOZWQY; and Tetsuo Kotani, "JIIA Strategic Comments (No. 6): The Multi-Domain Defense Force: Assessment and Challenges," Japan Institute for International Affairs, December 28, 2018, https://www2.jiia.or.jp/en/article_page.php?id=15.

JSDF cannot set up permanent joint task forces to respond to multidomain challenges in the East China Sea.[64]

In the realm of technology R&D, there are two challenges. One is the enduring cultural and normative barriers to leveraging R&D and basic research efforts in the civilian sector for military purposes. Despite the easing of defense equipment and technology transfer guidelines in 2014, a recent study shows that Japanese industries are concerned about being labeled as "merchants of death" for engaging in arms development.[65] From a business standpoint, the reputational cost of taking part in or expanding military-relevant R&D is too high for Japanese private technology firms and conglomerates with defense business segments, even though such segments only contribute to a fragment of their overall commercial sales.[66] The normative constraints are even greater in academic work. For instance, the Ministry of Defense's new funding mechanisms established in 2015 to support basic research in emerging dual-use technologies such as AI, quantum science, and robotics have not attracted academic institutions but instead have distanced them from military-relevant research. In 2017 the Science Council for Japan released a statement to reconfirm its position to not be engaged in military-related research, which de facto prohibited their involvement.[67] Accordingly, the number of academic institutions taking part in such programs has fallen significantly since then.[68]

Another challenge is the vulnerability of information security systems, including a lack of unified vetting processes for those involved in national security-related business. This undermines close coordination and cooperation among governments, industries, and universities. Former high-level U.S. officials have repeatedly called for Tokyo to adopt higher security protection mechanisms and to allow greater information sharing and cooperation in emerging technology development.[69] While the government considered the introduction of a security clearance mechanism in the economic security bill to strengthen technology protection, the item was left out in the final legislation for political reasons.[70]

Constitutional and legal constraints pose further challenges to the Japanese government's ability to enhance cybersecurity and intelligence-gathering efforts through civilian networks. For instance, Article 21 of the Japanese constitution prohibits government intervention in civilian networks. Article 4 of the Telecommunications Business Act further states the importance of "protection of secrecy" by mentioning that "[a]ny person who is engaged in a telecommunications business shall not disclose secrets obtained."[71]

---

64 "Jieitai ho" [Japan Self-Defense Forces Law], https://elaws.e-gov.go.jp/document?lawid=329AC0000000165.

65 Shahana Thankachan, "Japan's Security, Export Control and Arms Export Policy: Prospects for India-Japan Defence Cooperation," Delhi Policy Group, Policy Report, October 2020, 23, https://www.delhipolicygroup.org/uploads_dpg/publication_file/japans-security-export-control-and-arms-export-policy-prospects-for-india-japan-defence-cooperation-2085.pdf.

66 Alexandra Sakaki and Sebastian Maslow, "Japan's New Arms Export Policies: Strategic Aspirations and Domestic Constraints," *Australian Journal of International Affairs* 74, no. 6, (2020): 660.

67 "Statement on Research for Military Security," Science Council of Japan, March 24, 2017, https://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-s243-en.pdf.

68 Yuka Koshino, "Is Japan Ready for Civil–Military 'Integration'?" IISS, Analysis, August 3, 2021, https://www.iiss.org/blogs/analysis/2021/08/japan-civil-military-integration.

69 See, for example, "More Important Than Ever: Renewing the U.S.-Japan Alliance for the 21st Century," Center for Strategic and International Studies, October 2018, 9, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181011_MorethanEver.pdf.

70 "Japan Weighs Security Clearance System for Sensitive Economic Info," *Japan Times*, February 22, 2022, https://www.japantimes.co.jp/news/2022/02/22/national/japan-security-clearance-system.

71 "Telecommunications Business Act (Act No. 86 of December 25, 1984)," Ministry of Internal Communications (Japan), 2, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/pdf/090204_2.pdf.

Next Steps for U.S.-Japan Cooperation

Japan and the United States have strengthened bilateral coordination and cooperation at the strategic and practical levels, especially since the second Abe administration, through summits and bilateral and plurilateral mechanisms. These include the Japan-U.S. Security Consultative Committee (2+2) and space and cyber dialogues. From the standpoint of defense cooperation in cyber, space, and emerging technologies, the most significant development was the upgrade of the U.S.-Japan Defense Guidelines in 2015 for the first time since 1997. The new guidelines expanded cooperation at the policy and operational levels during peacetime and potential contingencies, including in the space and cyber realms.[72] The 2019 2+2 joint statement was important for improving deterrence because it affirmed "that international law applies in cyberspace and that a cyber-attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty." Nevertheless, questions remain as to which cases could amount to responses from the United States and Japan.

Under the Biden administration and the Suga and Kishida administrations, bilateral cooperation has made further progress. The joint statements from the 2021 2+2 and the April 2021 summit that followed were historic for mentioning the "importance of peace and stability across the Taiwan Strait," which contributed to opening public debate about Japan's role in a potential Taiwan contingency. The 2022 2+2 in January made further progress by committing to pursuing joint investments in critical and emerging defense technologies.[73] Most recently, the June 2022 Extended Deterrence Dialogue was an important step in sharing concerns and approaches to maintain and enhance the credibility of U.S. extended deterrence.[74]

Building on these efforts, the following options could be explored by the two countries to enhance both Japan's and the alliance's response capabilities and address the challenges arising from new domains and autonomous technologies.

Enhance Bilateral Coordination Mechanisms for Planning and Cross-Domain Operations

The two governments established the standing Alliance Coordination Mechanism under the U.S.-Japan Defense Guidelines in 2015 to "strengthen policy and operational coordination related to activities conducted by the Self-Defense Forces and the United States Armed Forces in all phases from peacetime to contingencies."[75] However, analysts, civilians, and military officers from both sides have expressed concerns about the effectiveness of the existing mechanism in the event of a high-end contingency in the East China Sea as well as Japan's lack of a counterstrike capability.[76] The shift to cross-domain operations, including in the new domains of space, cyber,

---

72 "The Guidelines for Japan-U.S. Defense Cooperation," Ministry of Defense (Japan), April 27, 2015, https://warp.da.ndl.go.jp/info:ndljp/pid/11591426/www.mod.go.jp/e/d_act/us/anpo/pdf/shishin_20150427e.pdf.

73 "Joint Statement of the U.S.-Japan Security Consultative Committee ('2+2')," U.S. Department of State, January 6, 2022, https://www.state.gov/joint-statement-of-the-u-s-japan-security-consultative-committee-22.

74 "U.S. Extended Deterrence Dialogue," Ministry of Foreign Affairs (Japan), Press Release, June 24, 2022, https://www.mofa.go.jp/press/release/press4e_003139.html.

75 "The Guidelines for Japan-U.S. Defense Cooperation."

76 See, for example, Scott W. Harold et al., "Japan's Possible Acquisition of Long-Range Land-Attack Missiles and the Implications for the U.S. Japan Alliance: Summary of a February 2021 Conference," RAND Corporation, 2022, https://www.rand.org/pubs/conf_proceedings/CFA1310-2.html.

and the electromagnetic spectrum, and the volume of data gathered through advanced ISR capabilities further complicate and challenge coordination.[77]

Some experts have called for the establishment of a joint C2 structure, modeled on the U.S.–South Korea alliance or NATO, once Japan obtains a counterstrike capability.[78] Given the existing burden on Japan's chief of staff of the Joint Office and its counterpart, the U.S. Indo-Pacific Command, the two sides could also improve coordination and prepare for a potential contingency in the Taiwan Strait by setting up a bilateral standing joint task force dedicated to high-intensity operations in the East China Sea.[79]

Engage Japan in the U.S.-Led Effort for Military Adoption of Emerging Technologies

Tokyo's pursuit of a multidomain defense concept, such as exists in the United States, China, the United Kingdom, and other countries, requires rapid development and military adoption of emerging and disruptive technologies. Japan's defense R&D is smaller than that of other major countries' militaries.[80] Bilateral efforts to cooperate on joint research in counter-hypersonic technologies and on a "proliferated low earth orbit satellite constellation" in the 2022 2+2 are intriguing signs of enhanced defense technology cooperation, but the extent to which the United States and Japan could cooperate in military adoption when it comes to joint investment in "critical and emerging fields, including artificial intelligence, machine learning, directed energy, and quantum computing" is unclear.[81]

Thus, exploring practical ways to involve Japan in other U.S. ally–led initiatives to develop joint capabilities, such as the Australia–United Kingdom–United States (AUKUS) partnership, could contribute to speeding up this process. Indeed, it could be too early to discuss Tokyo's direct engagement with AUKUS, as the specifics of the partnership are still unknown. However, materials released in April 2022 suggest that the target advanced capability areas (undersea capabilities, quantum technologies, AI, advanced cyber, hypersonic, counter-hypersonic, and electronic warfare) significantly overlap with ATLA's R&D priorities. The AUKUS parties are also reportedly interested in engaging with Tokyo, especially in the working group for counter-hypersonic technology.[82] Given that Japan has been deepening defense cooperation with Australia and the UK in recent years through joint training, exercises, and industrial cooperation, such consultation on developing a broader joint capability could benefit from a practical and interoperability standpoint.

Leverage the Private Sector for Defense

As the private sector is driving innovation in space, cyber, and autonomous technologies, both the U.S. and Japanese militaries are seeking to adopt civilian and commercial technologies to achieve a multidomain integration concept. This opens opportunities for cooperation between the high-tech firms in both countries. The two governments should leverage and encourage such

---

77 Harold et al., "Japan's Possible Acquisition," 26.

78 Ibid., 27.

79 See, for example, "More Important Than Ever"; and John P. Niemeyer, "U.S.-Japan Coordination in an East China Sea Crisis," *Asia Policy* 15, no. 3 (2020): 31–42.

80 Koshino, "Is Japan Ready."

81 "Joint Statement of the U.S.-Japan Security Consultative Committee ('2+2')."

82 "AUKUS sanka, Bei Ei Go ga Nihon ni dashin, goku cho onsoku heiki nado gijutsuryoku kitai" [The U.S., UK, and Australia Propose Japan to Join AUKUS: Expects Counter-Hypersonics Technology from Japan]," *Sankei Shimbun*, April 12, 2022, https://www.sankei.com/article/20220412-73VOZUMHBVKTFFHLLJHSZHUYQU.

industrial partnerships to enhance defense, especially to overcome normative challenges for businesses in Japan.

One example area would be the use of space and telecommunications technologies to enhance communications and ISR capabilities. The two governments are advancing their space cooperation by sharing SSA information through their militaries, but they could further leverage the existing capabilities and services in their commercial space sectors to gather, process, and share satellite imagery for regional security, especially in the maritime security domain.

Another example is cooperation in the military adoption of 5G. Both Japanese and U.S. forces are seeking to adopt 5G to improve their operational efficiencies, such as through increasing the speed of the data processing and decision-making required to build a multidomain force. Because 5G technologies are led by civilian firms, both countries' defense agencies have been calling for private telecommunications companies to explore potential ways to adopt them and conduct testing at their bases to measure performance.[83]

In the commercial telecommunications realm, some Japanese providers and operators are enhancing partnerships with U.S. firms to leverage technological innovation. For example, the Japanese company Rakuten is partnering with U.S. software-based firms to develop an end-to-end cloud-based, fully virtualized 5G system.[84] The two militaries could further utilize these partnerships to develop a C2 system to prepare for a multidomain operation.

Conclusion

The update of Japan's three defense strategy documents, growing public support for the country to take on greater regional and global security roles and responsibilities, and increasing security concerns arising from Chinese military modernization are creating momentum for Japan to enhance its defense capability and review its defense and security policies. The Kishida government is likely to enjoy a stable political base from which to pursue its ambition to "substantially reinforce" Japan's defense capability. However, given the above operational, constitutional, legal, and normative constraints, Tokyo cannot pursue these goals alone. While the LDP has called for defense spending of 2% of Japan's GDP, which is twice the existing budget, securing financial resources could take time.

The three steps discussed in the preceding section are key to contributing to and enhancing the effective deterrence and response capabilities of both Japan and the U.S.-Japan alliance, even when the prospect of a drastic spending increase could be politically difficult. To summarize, the first step is to enhance bilateral coordination between the United States and Japan to prepare for a potential contingency in the Taiwan Strait and to use Japan's newly adopted counterstrike capabilities, should the Japanese government decide to acquire such an option. The second step is to involve Japan in U.S. ally–led initiatives to cultivate joint advanced capabilities in support

---

[83] U.S. Department of Defense, "DOD Announces $600 Million for 5G Experimentation and Testing at Five Installations," October 8, 2020, https://www.defense.gov/News/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati; "Lockheed Martin and Verizon to Advance 5G Innovation for U.S. Dept. of Defense," Lockheed Martin, https://news.lockheedmartin.com/lockheed-martin-verizon-advance-5G-innovation-us-deptartment-defense; and Ministry of Defense (Japan), "Boeisho ni okeru jishojikken wo tomonau 5G chosa kenkyu ni shisuru: Joho teikyo no irai ni tsuite" [Request for Information That Contributes to 5G Survey Research Accompanying Demonstration Experiments by the Ministry of Defense], February 2021, https://www.mod.go.jp/j/procurement/chotatsu/naikyoku/koubo/2021/0212a.pdf.

[84] Yuka Koshino, "How the U.S. Can Promote Affordable Non-Chinese 5G in Asia," IISS, March 2020, https://www.iiss.org/blogs/analysis/2020/03/jc-5g-in-asia.

of Tokyo's effort to accelerate the military adoption of emerging and disruptive technologies. The third step is to leverage existing commercial industrial partnerships between the United States and Japan, especially in the realm of advanced communications technologies, to achieve multidomain integration and allow for enhanced defense.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

A Vietnamese Perspective on China's Military Modernization

Nguyen The Phuong

NGUYEN THE PHUONG is a Lecturer at Ho Chi Minh City University of Economics and Finance and a PhD candidate in maritime security and naval affairs at the University of New South Wales in Australia. He can be reached at <phuong.nguyen2@adfa.edu.au> or on Twitter <@Ng_Phuong91>.

EXECUTIVE SUMMARY

This essay examines China's advances in areas such as cyber technology, space-related capabilities, and autonomous systems and argues that they pose an increasingly asymmetrical threat to Vietnam's national security.

MAIN ARGUMENT

Vietnam's struggle against China's coercive behaviors has largely occurred in the maritime environment, with spillover effects in other critical domains. The huge technological gap between Vietnam and China makes things worse for the former, as new forms of warfare emerge. To limit any negative impact, Vietnam needs to recognize the importance of new technologies and their applications in the current security environment. This change in perception, moreover, must be accompanied by a rational and effective investment of resources focused on strengthening internal capabilities and taking advantage of existing international partnerships.

POLICY IMPLICATIONS

- Vietnam should develop its own strategic guidelines adopting and exploiting emerging technologies in the new security environment, especially in the maritime domain.
- Vietnam should strengthen bilateral cooperation with the U.S. in several areas such as building micro- and macro-satellites, developing autonomous systems for maritime security purposes, and conducting capacity building in cybersecurity. These initiatives should prioritize engagement with the private sectors and universities.
- The U.S. will need to be strategically patient toward Vietnam, especially in security and military cooperation. Although the relationship between the two countries has improved since 1995, trust-building mechanism should be enhanced through dialogues to mitigate strategic distrust.
- Vietnam and the U.S. should initiate joint cooperative programs through multilateral mechanisms. ASEAN-related mechanisms are obvious choices, but the U.S. can also draw on its expanded networks of allies and partners, especially key allies such as Japan, South Korea, and Australia that are Vietnam's traditional partners.

Vietnam's military strategies have always been dictated by several fundamental principles. Because the country is small in terms of power, these strategies are purely active-defensive in nature and will mostly employ an asymmetric approach in warfare. Its defense strategies are part of a broader "hedging approach" toward outside powers, which means Vietnam is basically neutral and will try its best to diversify its relationships with international partners and avoid wars. New technologies are playing an increasingly important role in redefining the security landscape in the Asia-Pacific, especially those relating to warfare. By addressing challenges, opportunities, and the security impact of technology with those principles in mind, Vietnam can better protect its national interests.

China has always been considered by Vietnamese political elites as the greatest threat to Vietnam's sovereignty and territorial integrity. This essay briefly reviews the key cyber, space, and autonomous weapons threats posed by the People's Republic of China (PRC) against Vietnam. It then discusses Vietnam's responses and areas of possible cooperation with the United States that could counter these threats.

Emerging Threats from China

Cyber- and Space-Related Threats

In terms of cyberthreats, Vietnam considers China's cyber capabilities as part of an overall approach to engage in economic and political coercion to maximize its influence and bargaining power. Hybrid warfare, including cyberoperations, is utilized not only by the government and the military but also by civilian groups. Civilian groups sponsored by the PRC government are useful in initiating low-profile attacks and sowing disinformation on Vietnam's social media (e.g., creating fake accounts). China's cyber capabilities, while still maturing compared to other cyber powers, are a concern for Vietnam and can still overwhelm its cyberdefense due to the sheer weight of China's human and financial resources and technological advantages.

Among the greatest concerns is that China may be able to attack critical cyberinfrastructure, especially as Vietnam is pushing to digitalize nearly every aspect of its social and economic activities. As an important example, two of the biggest international airports in Vietnam were attacked by hackers in 2016. Vietnamese state media announced later that the notorious Chinese hacker group 1937CN was the culprit. This group was also behind the massive cyberattacks against hundreds of Vietnamese websites during and after the HD-981 oil rig incident in the South China Sea in 2014. China may also disrupt the flow of information within Vietnam by attacking or blocking GPS systems or by sowing disinformation on various social media platforms. According to a report by We Are Social and Hootsuite, active social media users in Vietnam number 72 million, or nearly 74% of the country's population.[1] A distributed denial-of-service attack against public websites could disrupt access to critical and accurate information.

The most significant space threat, strategically and tactically, comes from China's satellite-based intelligence, surveillance, reconnaissance (ISR), navigation, and communications capabilities. In 2015, Vietnam failed to realize that China had in place a significant plan to upgrade its seven

[1] Simon Kemp, "Digital 2021: Vietnam," DataReportal, February 11, 2021, https://datareportal.com/reports/digital-2021-vietnam. YouTube, Facebook, and Zalo (a domestic firm) are the three platforms most used.

outposts in the Spratly Islands. This failure came in part because of a lack of robust maritime domain awareness (MDA) capabilities, including a 24/7 ISR network.

China has launched a range of satellites that have significantly enhanced its ISR capabilities, including space-based ISR, electro-optical ISR, synthetic aperture radar satellites, and electronic reconnaissance satellites. These systems introduce a range of capabilities of concern to Vietnam:

- improved long-range precision strikes within the South China Sea domain, which can threaten Vietnam's military maneuverability
- increased 24/7 ISR missions, which can jeopardize Vietnam's deployment of strategic military assets and enhance China's occupied positions in the South China Sea
- stronger assertion of de facto control in disputed territories, which means that China's positions in the South China Sea have become fortresses from which it can defend against Vietnamese attacks or launch attacks against Vietnamese outposts in the Spratly Islands with remarkable precision and coordination
- a strengthened network of MDA in the South China Sea encompassing the underwater, surface, air, and space domains

Autonomous System Threats

China's development of autonomous weapons systems has captured Vietnam's attention, from the manufacturing of those systems to their deployment in the field, especially within the maritime domain. The defeat of Armenia in the 2020 Nagorno-Karabakh war shows the importance of autonomous systems, especially drone warfare, on the battlefield.[2]

For Vietnam, the role of unmanned underwater vehicles in maritime warfare, as well as autonomous system swarm tactics, raises particular concerns. Although drones have been a means for small countries to effectively fight in low-intensity conflicts, big countries such as China can also exploit the advantages of these systems for both strategic and gray-zone operations. Vietnamese military observers have all agreed that the era of autonomous systems dominating battlefields has come, with significant development in both their theoretical use and their actual deployment on the battlefield. Strategically speaking, autonomous systems help China improve its control of the seas with multidomain power, where naval power is gradually transitioning from "surface ships" to "naval platforms." Naval warfare will be characterized by space and unmanned systems operating in support of naval platforms. Such warfare will also involve operations not only in the maritime domain but also in outer space, the air, subsurface, and the deep sea, where autonomous systems play an important role.

More concerning for Vietnam is what capabilities these autonomous systems have when they are deployed in peacetime scenarios by China. These activities include prepositioning naval forces, using naval deterrence or coercion, and controlling important sea lines of communication with these systems. Several gray-zone tactics have been observed through years of engagement with China and include the use of maritime law-enforcement forces to intimidate Vietnamese fishing vessels in disputed waters, the use of scientific vessels to explore waters within the PRC's nine-dash line, and the building of artificial islands in the Spratly Islands. Autonomous systems will help China increase the effectiveness of these activities. For example, a Chinese laboratory has built the

[2] Huynh Minh Chien, "Some Issues on Artificial Intelligence Warfare," *National Defense Journal*, January 27, 2022, http://tapchiqptd.vn/en/research-and-discussion/some-issues-on-artificial-intelligence-warfare/18251.html.

world's first unmanned ship capable of launching unmanned systems.[3] This ship will increase the collection of ocean data and improve the efficiency and level of observation, through which China can strengthen its MDA in the South China Sea.

Vietnam's Response

Cyber Threats

Vietnam's security mindset has always been focused on national interests, with regime survival as the top priority. It is therefore no surprise that Vietnam wants to extend its total control over cyberspace, especially over the internet, to achieve better control of its so-called cyber sovereignty.[4] The interaction among the state, its citizens, and the international community will play an essential role in increasing or decreasing the country's ability to manage cyberspace in the future.

Since 2005, Vietnam has promulgated various legal measures to strengthen the country's resilience in cyberspace and enhance its cybersecurity capability. The first holistic document that addressed cybersecurity dates back to 2010, with the release of a dedicated roadmap on digital information security development. Since then, other decrees, directives, and laws have been passed to strengthen Vietnam's security in cyberspace. None, however, has attained the level of a true national strategy on cybersecurity. More investment has been put into training specialists in cyberwarfare, increasing R&D, and enhancing the relationship between the public and private sectors in cyber areas. Another important aspect has been international cooperation, in which Vietnam seeks expertise from cyber powerhouses such as the United States, the United Kingdom, Japan, and Australia to access both know-how and technology, while also seeking cooperation to conform to international standards in the cyber realm.

To maximize its efforts in combating cybersecurity threats, the Vietnamese government must overcome several challenges, namely a lack of money, human resources, and modern technology access; the constant changing of cyberspace and related technologies; a lack of participation of different actors in society; and the limitation of regional and international cooperation in cybersecurity. More fundamentally, Vietnam must decide how to manage interactions between the state, its citizens, and the international community, as all will play an essential role in determining the country's ability to manage cyberspace. Vietnam needs to find ways to harmonize three contradictions: between cyber sovereignty and the unrestricted, interconnected spirit of the internet; between cyber sovereignty and human rights; and between cyber sovereignty and the involvement of multiple stakeholders in governance.[5]

One of Vietnam's long-standing challenges is its lack of human resources. As a result, cybersecurity-related education and training have become a priority for the Vietnamese government. According to a joint survey conducted in 2019 by the Ministry of Education and Training and the Ministry of Information and Communications, 37.5% of the total number of universities and colleges in Vietnam have courses related to information and communications

---

[3] "Quanqiu shou sou zhineng xing wu ren xitong muchuan xiashui" [The First Intelligent Unmanned Mothership Was Launched], STDaily.com, May 9, 2022, http://www.stdaily.com/index/kejixinwen/202205/09a3a9c6065b499caa34da2d4411a1d9.shtml.

[4] Van Thang Le, "An ninh thong tin o Viet Nam trong dieu kien hien nay—Van de dat ra va giai phap" [Information Security in Vietnam under Current Conditions—Issues and Solutions], Ministry of Public Security (Vietnam), 2019.

[5] Hao Yeli, "A Three-Perspective Theory of Cyber Sovereignty," *PRISM* 7, no. 2 (2017): 109–15.

technology (ICT), and 50,000 information technology students graduate each year.[6] In 2020, demand for ICT-related positions reached one million for the whole industry to be effectively developed, especially in the cybersecurity field, which means that Vietnam is facing a severe shortage of human resources. Additionally, a specialist from the Ministry of Education and Training noted that Vietnam is facing deficiencies in building and developing policies for ICT human resources.[7]

The constant evolution of cyberspace and related technologies is exacerbating many of the challenges facing Vietnam. R&D is required to play catch-up with the latest innovations in the field. Vietnamese universities and colleges need to invest more in R&D to improve their curriculum and attract students. Vietnam, as a developing country, must combine the promotion of ICT and the development of its digital economy with the security of its information systems and the structuring of a cybersecurity policy and strategy—all while receiving lower investment capacity than more industrialized countries.[8] Needing to play catch-up with a lack of financial resources is a major hurdle for Vietnam's cybersecurity and cyber capabilities. The Vietnamese government must be dynamic to reflect the evolution of cyberthreats and be flexible in designing technical and nontechnical standards.[9]

Vietnam has initiated an effective coordination strategy with other stakeholders, especially when adopting a more proactive position toward the private sector in the field of cybersecurity.[10] Large private companies like FPT Corporation, CMC Telecom, and Bkav have contributed significantly to the economic and business aspects of cybersecurity. But more must be done to expand the participation of other stakeholders, such as NGOs or independent think tanks, in the policymaking process. This will help Vietnam balance the interests between the state and the citizen and ease the contradiction between sovereignty and, to some extent, the concern about individual rights in cyberspace.

Much has been said about Vietnam's proactive attitudes in international cooperation on cybersecurity, not only by experts in the field but also from various legal documents that have been passed in recent years.[11] This cooperation has been explained through the perception that Vietnam is an underdog in the digital world. The country aspires to become a cybersecurity power, with its human resources being among the best in the world, according to Minister Nguyen Manh Hung from the Ministry of Information and Communications.[12] Recent developments have shown that Vietnam has slowly emerged as "the newest gladiator of cyberspace in the Asia-Pacific region": "Vietnamese-language based activity and internet traffic on the Dark Web are rising, and so are attacks on foreign multi-national corporations and organizations based in the

---

[6] Li Qing, "Nhan su nganh an ninh mang, du bao co hoi phat trien" [IT Human Resources in Vietnam: Potential Development], VietnamNet, April 16, 2019, https://vietnamnet.vn/vn/giao-duc/nhan-su-nganh-an-ninh-mang-du-bao-co-hoi-phat-trien-523787.html.

[7] Lê Quân, "Phat trien nhan luc cong nghe thong tin: Kho dem cua trong lo" [IT Human Resource Development: Hard to Quantify], *Bao Dau Tu*, March 7, 2020, https://baodautu.vn/phat-trien-nhan-luc-cong-nghe-thong-tin-kho-dem-cua-trong-lo-d117322.html.

[8] Candice Tran Dai, "Cybersecurity Governance Framework in Vietnam: State of Play, Progress and Future Prospects," *Asian Research Policy* 8, no. 1 (2017): 97.

[9] Ibid., 96.

[10] Ibid.

[11] Ibid., 97; and Hai Thanh Luong et al., "Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement," *International Journal of Cyber Criminology* 13, no. 2 (2019): 304–5.

[12] "Vietnam Aspires to Become a Power in Cybersecurity: Minister," *Nhan Dan*, April 16, 2019, https://en.nhandan.vn/vietnam-aspires-to-become-a-power-in-cybersecurity-minister-post72822.html.

country, particularly automotive companies and media houses."[13] The attack by the allegedly government-backed hacker group APT-32 on China's Ministry of Emergency Management and the government of Wuhan before and during the Covid-19 outbreak to compromise the professional and personal email accounts of those institutions' employees is a vivid example.[14] Another prominent incident was APT-32's effort to invade the networks of the Toyota and Hyundai corporations in 2019.[15] It is undeniable that Vietnam has become a cyberwarfare outpost. Future international cooperation, especially with other members of the Association of Southeast Asian Nations (ASEAN), must be constructed through an updated perspective in which Vietnam is now ready to play a more aggressive role in cyberwarfare and be a responsible stakeholder that abides by international law.

Space Threats

Unfortunately, Vietnam has not done much to counter China's advances in space-based ISR capabilities. Vietnam faces several fundamental obstacles to counterbalancing the PRC in this area, including a lack of resources, a slow-moving and sensitive-to-reform domestic defense industry, and suspicions toward the West among conservative elites, which hamper closer cooperation with countries such as the United States. These obstacles are not specific to Vietnam's developing space capabilities but also evident in other increasingly important aspects of warfare and technologies such as cyber and autonomous systems.

Vietnam's space capabilities are primarily in the civil realm. Initial research started in the 1980s, but serious R&D on satellite technology started gathering momentum in 2006 with the government's approval of the Space Technology Research and Development Strategy towards 2020. The goal was to bring Vietnam to an above-average level in the region, with the key objectives set as constituting legal policies to support space technology research and application; constructing space technology infrastructure; studying space exploration science and technology; and applying the resulting technologies. In 2011, the government established the Vietnam National Satellite Center, which operates under the Vietnam Academy of Science and Technology, to concentrate on the professional development and synchronization of infrastructure, technology skills, and human resources for satellite technology.

Vietnam has focused its resources on developing small satellites using synthetic-aperture radar, which provides high-resolution images and can operate in all weather conditions. Since 2013, Vietnam has also test-launched three small domestic satellites (the largest weighing 50 kilograms) into orbit with mixed results. Vietnam is not yet self-sufficient in satellite images and must rely on free images provided by international partnerships with the Japan Aerospace Exploration Agency, the European Space Agency, and the U.S. Geological Survey through Vietnam Data Cube—a satellite data-sharing system. These images and data have been extensively used for sustainable development (e.g., foresting, rice farming, and water monitoring).

---

[13] Abhilash Halappanavar, "Vietnam's Rise in Cyberspace," *Infosecurity Magazine*, June 22, 2020, https://www.infosecurity-magazine.com/next-gen-infosec/vietnam-cyberspace.

[14] Ankit Panda, "Offensive Cyber Capabilities and Public Health Intelligence: Vietnam, APT32, and COVID-19," *Diplomat*, February 24, 2022, https://thediplomat.com/2020/04/offensive-cyber-capabilities-and-public-health-intelligence-vietnam-apt32-and-covid-19.

[15] "Vietnam Hackers Attack the Email System of Toyota Corporate," VNetwork, December 31, 2019, https://vnetwork.vn/en/news/hacker-vietnam-tan-cong-email-doanh-nghiep-toyota.

Autonomous Systems

At present, autonomous systems have not been widely deployed by the Vietnamese military. Drone R&D in Vietnam took off in the early 2010s at a moderate pace and has concentrated on less technologically advanced parts such as engines, aerodynamic frames, and simple command-and-control systems. The circumstantial development of this game-changing but nascent technology in Vietnam raises four key issues.

First, it seems that prior to the 2010s, there was no implemented policy to coherently and comprehensively integrate drones into the general military strategy, and drones were mostly used as flying targets. Moreover, it remains unclear if there is any current doctrine that considers drones an integral part of defense strategy.

Second, due to the lack of policy supporting R&D on drones, there has been a dearth of financial resources to support these technologies, according to some experts.[16] Researchers confirmed that they did not receive the full funding promised by the government, and some even had to use their own financial resources to maintain projects. Although the demands for this kind of technology are huge and full of potential, research activities have nevertheless been sporadic and unsystematic.

Third, there was no systemic cooperation or coordination amongst different research groups conducting R&D on this new technology until 2017, which led to an infamous dispute between the Vietnam People's Air Defense–Air Force's Technical Academy and the Vietnam Academy of Science and Technology over which agency actually made the first Vietnamese drones.[17] This incident also revealed that although there was research about the theory of drones and their role in warfare, no agreed categories of drones had been laid out, and struggles probably took place between military and civilian research agencies over limited financial resources. This problem was partially solved in 2017 when Viettel Group and the Vietnam Academy of Science and Technology agreed to boost their cooperation, especially in several high-tech areas such as satellite technology, unmanned aerial vehicle (UAV) technology, and new material science.[18] However, this is part of the government's effort to improve Vietnam's science and technology capabilities in general and does not reflect a particular change in military policies to prioritize drone manufacturing.

Fourth, although heavily investing in efforts to build up and develop a strong domestic drone industry, Vietnam still relies on foreign countries for some types of drone technology. It is well-known that Israel was the first foreign partner that helped Vietnam develop UAVs (the first flying targets made by the Vietnam People's Air Defense–Air Force's Technical Academy were based on an Israeli variant). Vietnam subsequently received assistance from several other important partners, including Sweden (through a partnership with the Vietnam Aerospace Association), Belarus, and Russia. Foreign technologies are important in improving the capabilities and skills of Vietnamese researchers and technicians in making more advanced autonomous systems.

Vietnam has only been able to manufacture light and medium drones that focus on ISR missions and other civilian tasks. Making heavy drones with combat capabilities is a challenging task requiring generous investment, suitable human and technological resources, and political will. For urgent security needs, the Vietnamese military also imports, and receives in the form

---

16 "Viet Nam san xuat may bay khong nguoi lai tu bao gio?" [When Did Vietnam Start Making UAVs?], *Tuoi Tre*, May 14, 2013, https://tuoitre.vn/viet-nam-san-xuat-may-bay-khong-nguoi-lai-tu-bao-gio-548222.htm.

17 Ibid.

18 Thảo Lê, "Viettel hop tac cung VAST thuc day nghien cuu khoa hoc" [Vietnam and Vast Boost Cooperation in Scientific Research], *Nhan Dan*, March 28, 2017, https://nhandan.com.vn/khoahoc/item/32442802-viettel-hop-tac-cung-vast-thuc-day-nghien-cuu-khoa-hoc.html.

of military aid, several models of light UAVs from Israel and the United States, mostly for ISR missions.

Partnering with the United States

Vietnam has nominally the lowest level of partnership with the United States (a comprehensive partnership). In contrast, countries such as Japan, Australia, and the Philippines are U.S. treaty allies; India is a U.S. strategic partner; and Taiwan is an important U.S. traditional partner. Current relations between Vietnam and the United States, especially regarding security and defense, should not and cannot go too deeply into discussions about which weapons systems or assets are appropriate. Their history severely limits discussions of this kind. Most importantly, given the continuing strategic mistrust between the two countries, they must look for ways to strengthen mutual trust before bigger steps can be taken.

Technology is a special aspect of bilateral relations that can define the comprehensive partnership between Vietnam and the United States. However, technology is also a sensitive topic if it relates to military cooperation. Building trust is the main challenge for the military-to-military and defense relationship between the two countries. They could start by exploring several less sensitive areas, mostly dual-use, such as remote-sensing technology for maritime, environmental, and water management; space-related technology, such as developing micro- and macro-satellites to strengthen Vietnam's domestic capabilities in MDA; and artificial intelligence, machine learning, and other basic STEM subjects.

Other specific mechanisms for the Vietnam-U.S. partnership could include the following. First, Vietnam and the United States could continue to maintain an official dialogue (Track 1) on defense and technological development for dual-use purposes (including between Vietnam's Ministry of Foreign Affairs, Ministry of Defense, and Ministry of Science and Technology and their U.S. counterparts) and gradually explore opportunities to deepen cooperation on technology (e.g., through space cooperation or the introduction of technological means to increase MDA capabilities). However, Vietnam will consider some areas of cooperation to be too sensitive, such as sharing intelligence as part of a technology-sharing scheme.

In addition, both countries could continue to sponsor programs to raise awareness among Vietnamese officials and academics about the role of technology in improving national security (e.g., technologies related to MDA, space-based ISR, autonomous systems, and nonproliferation). These programs should also be open to universities (through exchanging officials and scholars or engaging with Vietnamese scholars in various Track 2 dialogues and initiatives) and can cover the role of GPS and other related technologies in expanding MDA capabilities at sea; the role of drones and other autonomous and semi-autonomous systems, in both tactical and strategic terms (i.e., how a small country like Vietnam uses drones to best suit its interests); cybersecurity and cyberwarfare in the new era, especially in hybrid warfare (i.e., how Vietnam can effectively cope in an asymmetrical environment); and international legal standards in cyber, space, and autonomous realms, including managing emerging technologies in warfare.

Educational cooperation between the two countries is a hallmark of the comprehensive partnership and brings about long-term strategic benefits for both sides. One priority should be to initiate programs or funding that can help universities or technological institutes jump-start their R&D on key technologies. Another priority is to provide scholarships and other educational

and training support to strengthen human resource development in STEM or other technological areas for Vietnamese students in select universities.

Moreover, Vietnam and the United States should initiate joint cooperative programs through multilateral mechanisms (including through ASEAN or strategic partners of both countries such as Japan, South Korea, Australia, and India). Such programs should include a civil space dialogue, as the United States has initiated similar bilateral dialogues with several members of ASEAN. These could be transformed into a multilateral dialogue. Similar mechanisms could also be established for other technological areas, including cybersecurity, autonomous systems, and nonproliferation. For example, a cyber forum could be organized annually by a joint effort of the United States, the UK, and Australia that includes all ASEAN states. Although Vietnam lacks the resources to maintain the same level of awareness as China, there is the option to work with other like-minded countries in ASEAN (e.g., the Philippines, Indonesia, and Singapore) to develop ISR capabilities. There is also the possibility of bilateral technology transfers with more technologically advanced countries such as Singapore, Japan, South Korea, or India.

Similarly, Vietnam and the United States should consider expanding the current MDA initiative to include other countries both inside and outside ASEAN. It can not only focus on technological matters but possibly include intelligence sharing and coordination hubs that cross the civil-military and public-private divides.

Conclusion

Vietnam's main strategic concern since the end of the 2000s has always been the South China Sea. China's increasing investment in new military technologies and their application in the maritime domain within the first island chain has garnered special attention from Vietnam's strategists and military observers. None of the cyber, space, and autonomous weapons threats from China's military modernization that are discussed in this essay have been sufficiently addressed in terms of operational doctrine or weapon procurement strategy. The reasons for this range from a lack of essential resources such as money or human capital to outdated thinking or infighting between different interests in R&D. The biggest hurdle, however, could be the lack of understanding of the need to modernize the Vietnam People's Army in comprehensive and innovative ways that leave behind the old Soviet-style structural problems, just as China has done.

In particular, lessons learned from recent incidents in the South China Sea prove that if Vietnam had better MDA capabilities, China's land reclamation in the Spratly Islands would have been prevented or at least slowed. The inability to detect what China has been doing in the waters around the islands since 2015 proves that Vietnam does not possess the capability to monitor the disputed waters and its exclusive economic zone (EEZ) around the clock, hampering an effective response.

Vietnam should develop its own strategic guidelines and have them integrated into the country's maritime security strategy. At present, MDA is a new operational concept within the military and has not been thoroughly researched. A comprehensive MDA includes both "soft" and "hard" components that will help identify, locate, and track potential threats in the maritime arena as well as provide the ability to persistently monitor the maritime domain. Recently, Vietnam has assured better MDA by modernizing its maritime law-enforcement agencies, notably the Vietnam Coast Guard and the Vietnam Fisheries Resources Surveillance. Besides the Vietnam People's Navy and

the maritime militia, these two agencies help strengthen the country's presence in disputed waters, enforce its EEZ, intercept illegal fishing, and counter smuggling and piracy.

Unlike the other five countries covered in this report, Vietnam is not a strategic partner or traditional ally of the United States. The two countries do not have a strong historical bilateral military foundation. Due to the legacy of war and strategic distrust between them, it is important to appreciate that measures to increase trust are the core catalyst for any meaningful cooperation to take root. This is not to say that deeper military cooperation is impossible, but it must be designed to increase the level of trust between the two countries as much as possible.

Cooperation on military technology is a sensitive issue, which is why Vietnam always chooses traditional partners (like Russia or Eastern European countries) to help in R&D or procurement. However, there are gaps that the United States or other Western countries can fill. In particular, space, cyber, and autonomous systems developed by the West are more advanced and reliable and offer opportunities for closer cooperation.

More generally, the United States needs to apply a gradual and patient approach regarding military cooperation with Vietnam and concentrate on "soft" initiatives such as training, knowledge sharing, or Track 2 activities. Moreover, Vietnam will feel more assured when military cooperation is done through multilateral channels, be it through ASEAN-related mechanisms or other, newer, minilateral initiatives.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #103 | DECEMBER 2022

Philippine Security Implications from China's Autonomous, Cyber, and Space Weapons Systems

Francis C. Domingo

FRANCIS C. DOMINGO is Associate Professor of International Studies at De La Salle University in Manila. He can be reached at <francis.domingo@dlsu.edu.ph> or on Twitter <@frcdlive>.

EXECUTIVE SUMMARY

This essay explores the implications of the use of established and emerging technologies by the People's Republic of China (PRC), the Philippines' limited response in countering the PRC's activities, and opportunities for enhancing cooperation with the U.S.

MAIN ARGUMENT

The PRC's efforts to harness the advantages of established and emerging technologies pose a serious threat to the national security of the Philippines. The PRC's autonomous weapons systems, while still underdeveloped, can enhance the scope and effectiveness of air and maritime operations in the South China Sea. Its cyber capabilities have been instrumental in collecting national security secrets of different states in the region. Finally, the PRC's evolving space and counterspace weapons signal the country's technological superiority over weaker states. Given the security implications of the PRC's use of autonomous, cyber, and counterspace weapons, the Philippines needs to leverage its alliance with the U.S. if it intends to increase its capacity to defend against complex Chinese threats.

POLICY IMPLICATIONS

- The Philippines should leverage its alliance with the U.S. to counter the security threats posed by the PRC.
- The U.S. can help the Philippines' defense posture by focusing military assistance on enhancing intelligence, surveillance, and reconnaissance capabilities and strengthening the land-based missile forces.
- The U.S. can support the Philippines' engagement with international institutions by collaborating on the promotion of cyber norms and agreeing on a common position regarding autonomous weapons systems.

The rapid modernization of the armed forces of the People's Republic of China (PRC) is driven in part by the belief that its military forces should play a more prominent role in advancing the country's foreign policy interests. In this regard, a fundamental goal of the People's Liberation Army (PLA) is to protect the PRC's security interests against other states by deploying emerging and established military technologies such as autonomous weapons systems, cyber weapons, and counterspace weapons.

While the PRC is focused on developing global power-projection capabilities, less capable states like the Philippines are still in the process of enhancing their ability to detect and respond to technology-enabled threats to national security. In this context, this essay explores the security implications of the PRC's use of autonomous, cyber, and counterspace weapons on the Philippines. It argues that the Philippines needs to leverage its alliance with the United States if it intends to increase its capacity to defend against complex Chinese threats.[1]

This essay will briefly address these developments in three principal parts. The first section explores the PRC capabilities and threats of greatest concern to the Philippines in relation to cyber, counterspace, and autonomous weapons. The next section examines Philippine military responses in relation to emerging and established military technologies in the PLA arsenal. The third section then proposes mechanisms that the Philippines can adopt together with the United States to counter the complex national threats posed by the PRC.

Emerging PRC Capabilities and Threats

Cyber- and Space-Related Threats

Intelligence collection through cyberspace. China views cyberspace as a domain vital to "national security, economic growth and social development," but it is also viewed as a significant source of competition and conflict.[2] In this regard, the PLA has exploited cyberspace for intelligence collection, systematically targeting government agencies, private corporations, and international organizations in the Philippines for at least twelve years. Since the PLA's cyberespionage campaigns are well-documented, a summary of cases that involve the Philippines is instructive for this essay.[3]

The first case is a malware-based cyberespionage network designated as GhostNet, which was discovered by the SecDev Group and the University of Toronto in 2009. Computers in the Philippine Department of Foreign Affairs and the Department of Science and Technology were exploited by the PLA to collect intelligence in support of Chinese defense and security policy.[4] The second case is a cyberespionage operation classified as Lotus Blossom and reported by Palo Alto Networks in 2015. The PLA collected sensitive information relating to high-level officials from

---

[1] An autonomous weapons system is a system that, "once activated, can select and engage targets without further intervention by a human operator." See U.S. Department of Defense, "DoD Directive 3000.09: Autonomy in Weapon Systems," November 21, 2012, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf; and Elsa B. Kania, "'AI Weapons' in China's Military Innovation," Brookings Institution, Global China, April, 27, 2020, https://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation.

[2] State Council Information Office of the People's Republic of China (PRC), *China's National Defense in the New Era* (Beijing, July 2019), https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

[3] China's cyberoperations against the Philippines can be classified as espionage and vandalism (website defacements). Incidents of vandalism are not discussed in this essay since attribution to China was not established. For reference, see Miguel Alberto Gomez, "Intrinsic or Opportunistic: Chinese Cyber Espionage Strategies," *National Cybersecurity Institute Journal* 2, no. 1 (2015): 5–11; and Mark Manantan, "The Cyber Dimension of the South China Sea Clashes," *Diplomat*, August 5, 2019, https://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes.

[4] Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," SecDev Group and Citizen Lab, March 29, 2009, available at https://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

the Philippine Department of Foreign Affairs and the Armed Forces of the Philippines (AFP).[5] The third case is a cyberespionage operation described as APT 40 and reported by FireEye in 2019. The PLA collected intelligence on engineering, transportation, and defense industries in the Philippines in support of China's naval modernization.[6] Despite the systematic espionage operations against the Philippines, there are no reports of outcomes that impeded the ability of the military or intelligence agencies to protect the country's national interests.

Evolving outer space capabilities. The PRC considers outer space a critical domain for strategic competition. It has dedicated significant economic and political resources to strengthen its space-related technologies to allow for greater power projection. In at least two cases, China has successfully demonstrated its space and counterspace capabilities. The first case is the anti-satellite test in 2007 when the country used its anti-satellite missile (the SC-19) to destroy a weather satellite.[7] The second is a more recent case when the PRC tested a hypersonic missile that traversed the Earth in low orbit before missing its target by several miles.[8]

These tests signal China's technological superiority over less capable states in the region, but there is no evidence to suggest that the Philippines is directly threatened by PRC outer space capabilities or active engagements in outer space. Indeed, the latest agreement between the Department of National Defense and the Philippine Space Agency (PhilSA) facilitates their collaboration in four areas: (1) knowledge exchange regarding space science and technology applications, (2) capacity building in the application of satellite-based technologies, (3) research and development activities, and (4) public engagement (conferences, symposia, and workshops).[9] To be more specific, the agreement intends to improve the AFP's maritime domain awareness, area surveillance, and monitoring. These initiatives relate to protecting territorial integrity in the West Philippine Sea in general, rather than countering space-related or other threats from the PRC.

Emerging Autonomous Weapons Threats

The global competition for the use of emerging technologies in military affairs is escalating, with the PRC aiming to become a "global innovation superpower."[10] The PLA is still in the process of developing autonomous weapons systems, and there has been progress in at least two areas of military operations. The first is the application of artificial intelligence in command and control. The Central Military Commission's Joint Staff Department has tasked the PLA to advance "intelligentized command decision-making," with the objective of limiting human involvement in decision-making during military operations.[11] The second is the PLA Navy's experiments involving

---

[5] Robert Falcone et al., "Operation Lotus Blossom," Palo Alto Networks, June 16, 2015, https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.

[6] Fred Plan et al., "APT40: Examining a China-Nexus Espionage Actor," FireEye, March 4, 2019, available at https://www.mandiant.com/resources/blog/apt40-examining-a-china-nexus-espionage-actor.

[7] Carin Zissis, "China's Anti-satellite Test," Council on Foreign Relations (CFR), February 22, 2007, https://www.cfr.org/backgrounder/chinas-anti-satellite-test.

[8] Demetri Sevastopulo and Kathrin Hille, "China Tests New Space Capability with Hypersonic Missile," *Financial Times*, October 16, 2021, https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb.

[9] Jerome Siacor, "The Philippines Leverages Space Tech for National Defence," OpenGov Asia, April 19, 2022, https://opengovasia.com/the-philippines-to-max-on-space-tech-to-exert-nations-sovereignty; and Cristina Arayata, "How Could Space Tech Help Protect One's Territory?" March 10, 2022, https://www.pna.gov.ph/articles/1169515.

[10] Michael C. Horowitz and Lauren A. Kahn, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," CFR, November 4, 2021, https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape.

[11] Elsa B. Kania, "Chinese Military Innovation in the AI Revolution," *RUSI Journal* 164, no. 5–6 (2019): 26–34.

autonomous underwater vehicles, "including those that might be used in combat operations, while also concentrating on data fusion to improve maritime situational awareness."[12]

The PLA's development of autonomous weapons systems presents a threat to the national security of the Philippines for three reasons. First, the use of autonomous weapons systems can act as a force multiplier to the PLA's already overwhelming conventional military forces. Second, their use can strengthen the position of the PLA in the contested areas of the South China Sea by lowering the risk of casualties in conflicts. Third, the use of autonomous weapons systems is a threat to the Philippines because the AFP does not have existing measures to counter them.

The Philippines' Strategy: Building a Minimum Credible Defense Posture

The AFP is expediting the development of a minimum credible defense posture to enhance its overall capacity to defend the national security of the Philippines.[13] The AFP needs to strengthen its conventional military capabilities before it can effectively counter the PLA's autonomous, cyber, and counterspace weapons.[14] Indeed, at the time of writing, Russia's invasion of Ukraine has not dissuaded the Philippines from purchasing Russian Mil Mi-17 heavy-lift helicopters because defense officials believe that the Philippines will not be penalized for pursuing such a deal.[15] In this regard, Philippine national security agencies have focused on two initiatives: developing military cyber capabilities and building the capacity to observe the space activities of other states. Despite their significance, autonomous weapons systems are not discussed in this section because there is no clear evidence to confirm that the AFP is considering the use of such weapons as part of its fifteen-year modernization program. Indeed, they are barely mentioned in the country's most recent national security strategies.[16]

Securing Cyberspace

Cybersecurity continues to be an emerging security issue in the Philippines. The government considers the PRC's cyberoperations a threat to national security, but that is not the primary reason the Philippines is building its cyber capabilities.[17] The PLA has targeted the country since 2009, but government initiatives to secure national assets only intensified when the *National Cybersecurity Plan 2022* was implemented.[18] In this sense, the protection of critical information infrastructure from hacktivists and criminals is the main driver for enhancing cyber capabilities.

---

12 Kania, "Chinese Military Innovation in the AI Revolution," 31–32.

13 For the purposes of this essay, minimum credible defense is defined as "maintaining proportionate defensive military capabilities to protect national sovereignty within a projected period to enable the arrival of military reinforcements of allied states." See Francis C. Domingo, "The Contexts of Strategy as a Guide for Defense Planning in the Philippines," *Defense and Security Analysis* 31, no. 2 (2015): 159–67.

14 Francis C. Domingo, "Missiles Not Rifles: The Significance of Military Modernization for the Next President," Ballots and Bullets, April 13, 2016, https://nottspolitics.org/2016/04/13/missiles-not-rifles-the-significance-of-military-modernization-for-the-next-president.

15 David Santos, "PH-Russia Chopper Deal Still a Go Despite Ukraine War," CNN Philippines, March 9, 2022, https://www.cnnphilippines.com/news/2022/3/9/ph-russia-chopper-deal-pushing-through.html.

16 See, for example, Office of the President (Philippines), *National Security Strategy 2018* (Manila, July 2018), available at https://mb.com.ph/2018/07/08/national-security-strategy-2018; Department of National Defense (Philippines), *National Defense Strategy 2018–2022* (Quezon City, October 2018); and Armed Forces of the Philippines, *National Military Strategy 2019* (Quezon City, 2019).

17 Miguel Alberto Gomez, "Establishing a Philippine Cyber Command: Points to Consider," East Asia Forum, December 14, 2012, https://www.eastasiaforum.org/2012/12/14/establishing-a-philippine-cyber-command-points-to-consider.

18 Francis C. Domingo, "Strategic Considerations for Philippine Cyber Security," Stratbase ADR Institute for Strategic and International Studies, Occasional Paper, no. 9, January 2016.

In responding to cyberthreats, the Department of Information and Communications Technology is the lead agency for managing all cybersecurity initiatives. The Philippine National Police and the National Bureau of Investigation are the main agencies for countering cybercrime, while the AFP takes charge of "national cyber defense," which involves securing all military networks and systems as well as collecting threat intelligence on adversaries.[19] The newly established AFP Cyber Group is therefore the best government unit to respond to the PLA's cyber intrusions, particularly during exchanges related to territorial disputes in the South China Sea.[20]

The cyber capabilities of the Philippines are still in their formative stages. The government has implemented most of the initiatives that it presented in the *National Cybersecurity Plan 2022*, but there are at least three policy issues that must be addressed.

The first is the need to consider state-sponsored cyberoperations as a national security threat to the Philippines. Cyberoperations conducted by states are not currently considered a national security threat by the government. For instance, the *National Security Policy 2017–2022* and the *National Security Strategy 2018* classify crimes such as computer-related fraud, child pornography, and computer-related identity theft as the main threats in cyberspace.[21]

The second is the need for the government to manage the widening technology-policy gap. Cybersecurity initiatives in the Philippines are still directed by technologists from the government and private sector, with limited engagement from the defense and law-enforcement communities. The initiatives are therefore focused on strengthening the technical and operational aspects of cybersecurity, such as through the adoption of the ISO/IEC 27001 family of standards for information security, the establishment of a national computer emergency response team and the Philippine National Public Key Infrastructure, and other technical measures.[22] The technology-policy gap affects the coordination of cybersecurity initiatives because the purpose of implementing technical measures and the policy outcomes that the government intends to achieve are not always aligned.[23]

The third policy issue is the need for the government to include cybersecurity in the Philippines' foreign policy agenda.[24] The Department of Foreign Affairs has contributed to several regional and global initiatives to secure cyberspace, such as the development of the *ASEAN Cybersecurity Cooperation Strategy (2021–2025)* and the creation of global cyber norms through the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[25] However, diplomatic initiatives are not yet considered part of the cybersecurity measures implemented by the government. Indeed, the Department of

---

19 Department of Information and Communications Technology (Philippines), *National Cybersecurity Plan 2022* (Quezon City, May 2017), https://dict.gov.ph/national-cybersecurity-plan-2022.

20 Manantan, "The Cyber Dimension of the South China Sea Clashes."

21 For an extensive list of cybercrime offenses in the Philippines, see Congress of the Philippines, "Republic Act No. 10175: Cybercrime Prevention Act of 2012," September 12, 2012, https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175.

22 The ISO/IEC 27001 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognized framework for best-practice information security management. See International Organization for Standardization, "ISO/IEC 27001 Information Security Management," https://www.iso.org/isoiec-27001-information-security.html; and "Cybersecurity in the Philippines: Global Context and Local Challenges," Asia Foundation, Secure Connections, March 14, 2022, https://asiafoundation.org/publication/cybersecurity-in-the-philippines-global-context-and-local-challenges.

23 See, for example, Lian Buan, "DICT's Unspent P300-M Budget for Projects Went to Intel Fund," Rappler, February 3, 2020, https://www.rappler.com/nation/250897-dict-unspent-budget-projects-went-to-intelligence-fund.

24 Francis C. Domingo, "Cybersecurity and the Foreign Policy of the Philippines," 9DashLine, June 26, 2020, https://www.9dashline. com/article/cybersecurity-and-the-foreign-policy-of-the-philippines.

25 Association of Southeast Asian Nations, *ASEAN Cybersecurity Cooperation Strategy (2021–2025)* (Jakarta, February 2021), https://asean.org/our-communities/economic-community/asean-digital-sector/key-documents.

Foreign Affairs is not even considered a stakeholder in securing national interests in cyberspace based on the *National Cybersecurity Plan 2022* or in other high-level national security documents published by the government.

Capacity Building for Space Operations

The Philippines signified a stronger interest in developing more elaborate space capabilities through the creation of PhilSA in 2019. Aside from research, capacity building, and education, a core mandate of the agency is to strengthen the national security of the Philippines. Specifically, one of its objectives is "to ensure access to space and its environs as a sovereign right in the promotion of national security towards the attainment and protection of national interest."[26]

In this regard, the Philippines has launched two Earth observation satellites, the Maya-1 in June 2018 and the Diwata-2 in October 2018.[27] Although national security is one of PhilSA's key development areas, there is no evidence to suggest that the observation satellites were deployed in response to China's space operations. Instead, PhilSA appears to have been established to improve the government's capacity to monitor natural resources, mitigate natural disasters, and enhance maritime domain awareness.[28] There are two points that support these claims. First, the Philippine government has assured the public that it does not consider the PRC's space operations a direct threat to national security.[29] Second, the AFP continues to focus on internal security issues despite the commitment to shift to external defense.

Partnering with the United States

Reviewing the Philippine-U.S. Alliance

The most logical strategy for countering the complex security threats posed by the PRC is still for the Philippines to leverage its alliance with the United States. A crucial task moving forward is for both states to evaluate whether the security guarantees stipulated in the 1951 Mutual Defense Treaty can address security threats posed by cyber and outer space operations. In terms of cyberoperations, the alliance should clarify whether the United States is obligated to respond to a cyberattack against critical information infrastructure in the Philippines, considering that cyberattacks often do not have any kinetic effects.

If the interpretation is that the treaty does not cover cyberattacks, then the alliance can discuss other options such as diplomatic protests and "naming and shaming" tactics that can impose a reputational cost on the PRC.[30] As for outer space operations, the alliance should determine how the Philippines can invoke the treaty when it has yet to develop the capacity to detect and

---

26 PhilSA, "About PhilSA," https://philsa. gov.ph/about.

27 PhilSA, *Our Place in Space*, vol. 1, Space Data Mobilization (Quezon City, October 2020), https://philsa.gov.ph/our-place-in-space-volume-1.

28 Ibid.

29 PhilSA director general Joel Marciano Jr. assured the public that the Long March 5 rocket, which was launched by China in November 2020, was intended for a "peaceful space mission intended to collect lunar samples, which can contribute to scientific knowledge." See Timothy James Dimacali, "China Moon Rocket Flies Over Luzon, Sparks Security Concerns," ABS-CBN News, November 25, 2020, https://news.abs-cbn.com/spotlight/11/25/20/china-moon-rocket-flies-over-luzon-sparks-security-concerns; and Gabriel Pabico Lalu, "PH Won't Go to War with 'Good Friend' China, Says Duterte," *Philippine Daily Inquirer*, April 28, 2021, https://newsinfo.inquirer.net/1425037/meron-tayong-utang-na-loob-duterte-says-china-a-good-friend-ph-wont-go-to-war.

30 Stephanie Carvin, "The Name, Blame, Shame Game: Are Cyber Attributions Useful?" Centre for International Governance Innovation, July 28, 2021, https://www.cigionline.org/articles/the-name-blame-shame-game-are-cyber-attributions-useful.

monitor hostile activities in the Earth's atmosphere and orbit. Is the United States willing to share intelligence if there are potential space-related threats to the Philippines? These are some of the issues that need to be considered when reviewing the Mutual Defense Treaty.

Building Military Capacity

The Philippines receives an average of $125 million annually from various military assistance programs offered by the United States.[31] While these resources are typically allotted for strengthening conventional military capabilities, several capabilities are critical for the AFP's ability to respond to complex security threats.

First, the United States can help the Philippines by focusing assistance on enhancing intelligence, surveillance, and reconnaissance (ISR) capabilities that are crucial for detecting and monitoring the deployment of autonomous weapons systems in the South China Sea. Since ISR capabilities can be utilized for different purposes, the development of these capabilities must be managed through official agreements (e.g., the Enhanced Defense Cooperation Agreement) and with oversight from the Philippine Congress. Second, the United States can help by focusing assistance on strengthening land-based missile forces to supplement the BrahMos cruise missiles purchased from India, given the extensive coastline of the Philippines.[32] Third, building on the previous section, the United States can lobby the Philippine government to prioritize cyberspace as a defense priority. While the United States considers state-sponsored cyberoperations to be a significant threat, they are not given the same importance in the Philippines. In addition, the United States can also help the AFP develop the capacity to operate in cyberspace through training exercises such as Cyber Flag 21-1 and Cyber Storm.[33] The focus of these exercises needs to be on strengthening computer network defense and hardening critical infrastructure.[34]

Supporting Research on National Security

The AFP needs to strengthen its capacity for research if it wants to effectively respond to complex threats. Its current strategies and policies are not necessarily informed by research produced within or outside the national security community.[35] Although research on emerging technologies is prolific in the Philippines, the outcomes usually focus on the technical aspects of the complex security threats, making it challenging for policymakers to draw implications for strategy and policy.[36] Moreover, there are currently few local organizations (public or private) that specialize in research on the implications of autonomous weapons systems, cyberoperations, or even space weapons in the Philippines. The United States can support the research and development efforts of the Philippines by increasing interdisciplinary research engagement through joint research projects, workshops, and continuing education.

---

31 U.S. International Trade Administration, "Philippines—Country Commercial Guide: Defense," September 11, 2021, https://www.trade.gov/country-commercial-guides/philippines-defense.

32 Priam Nepomuceno, "BrahMos Ideal Weapon for Navy Missile Project," Philippine News Agency, March 20, 2021, https://www.pna.gov.ph/articles/1133128.

33 "DoD's Largest Multinational Cyber Exercise Focuses on Collective Defense," U.S. Department of Defense, Press Release, December 6, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense; and U.S. Cybersecurity and Infrastructure Security Agency, "Cyber Storm 2020: After-Action Report," August 2020, https://www.cisa. gov/sites/default/files/publications/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf.

34 Nepomuceno, "BrahMos Ideal Weapon for Navy Missile Project."

35 "Mapping Expertise on Strategic Studies," University of the Philippines, Center for Integrative and Development Studies, December 2018.

36 See, for example, Melvin Gascon, "Senators Alarmed Gov't Helpless to Counter Cyberthreats," *Philippine Daily Inquirer*, December 8, 2020, https://newsinfo.inquirer.net/1369152/senators-alarmed-govt-helpless-to-counter-cyberthreats.

Engaging International Institutions

Since the Philippines is less capable than some neighboring countries, such as the PRC, it has strengthened its engagement with international partners to supplement its military modernization through bilateral security cooperation. There are two areas where the United States can help the Philippines.

The first is promoting the UN cyber norms. The United States can support the diplomatic protests of the Philippines if and when the PRC breaches cyber norms and targets critical infrastructure or neglects the misuse of information technology by Chinese hacktivists, especially during incidents that relate to territorial disputes in the South China Sea. There are at least two previous cases that involve hacktivism and territorial disputes. One case was a series of exchanges (i.e., website defacements and denial-of-service attacks) between Chinese and Philippine hackers as a reaction to the standoff between China Marine Surveillance and the Philippine Navy at Scarborough Shoal in April 2012.[37] A more recent case was the cyber intrusions against multiple Philippine government websites after the Permanent Court of Arbitration ruling that invalidated the PRC's claims in the South China Sea in 2016.[38]

The second area is agreeing on a common position regarding autonomous weapons systems. A consensus is emerging in the international community that the use and production of autonomous weapons systems should be restricted on ethical (targeting based on sensor inputs rather than human beings) and legal (no measures to ensure human control) grounds.[39] While both states have not supported the proposal to ban the use of autonomous weapons, it is not clear if they are inclined to support the development and use of these weapons in the future.[40] Because the United States and the Philippines are security allies, reaching a common understanding regarding the use of autonomous weapons systems is crucial in case the PRC deploys these weapons in the coming years.

Conclusion

The PLA's use of established and emerging technologies has yet to be considered a serious threat to the national security of the Philippines. The PLA's development of autonomous weapons systems may be a serious concern for states in the region, but there is no evidence to suggest that the AFP is considering the development of similar systems within the next decade. The PRC's evolving space and counterspace weapons have caught the attention of the United States, but government officials in the Philippines have downplayed potential threats related to outer space operations. On the other hand, the Philippines regards the PLA's cyberoperations as a threat because they have been instrumental in collecting national security secrets of different states in the region.

Despite these emerging threats, the Philippines has not responded directly to the PRC's military transformation efforts. There is no evidence to suggest that the AFP is preparing for the deployment

---

37 Adam Segal, "China-Philippines Hacking War: A Missed Opportunity for Beijing?" CFR, May 10, 2012, https://www.cfr.org/blog/china-philippines-hacking-war-missed-opportunity-beijing.

38 Janvic Mateo, "68 Gov't Websites Attacked," *Philippine Star*, July 16, 2016, https://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked.

39 Adam Satariano, Nick Cumming-Bruce, and Rick Gladstone, "Killer Robots Aren't Science Fiction. A Push to Ban Them Is Growing," *New York Times*, December 17, 2021, https://www.nytimes.com/2021/12/17/world/robot-drone-ban.html.

40 Mary Wareham, "Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control," Human Rights Watch, August 10, 2020, https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and.

of autonomous weapons systems. The Philippines has implemented a comprehensive response to manage cyberthreats, but these initiatives were implemented years after the PRC started targeting government agencies and private companies. In terms of outer space operations, it is clear that the justification for creating PhilSA is primarily to enhance the capacity of the government to monitor natural resources, mitigate natural disasters, and enhance maritime domain awareness rather than to respond to PRC space and counterspace capabilities.

The logical strategy for countering the complex security threats posed by the PRC is for the Philippines to leverage its alliance with the United States. This essay proposes four mechanisms that can help the Philippines defend against these threats with U.S. assistance. First, both states need to evaluate whether the security guarantees stipulated in the 1951 Mutual Defense Treaty can address security threats posed by cyber and outer space operations. Second, the United States can help the Philippines build military capacity by enhancing ISR capabilities, strengthening land-based missile defenses, and developing its capacity for cyberoperations through training exercises. Third, the United States can support the Philippines' research and development efforts in the areas of autonomous, cyber, and counterspace weapons by increasing interdisciplinary engagement. Fourth, the United States can support the Philippines in engaging international institutions by promoting the UN cyber norms and working to find a common position regarding autonomous weapons systems.

Seattle and Washington, D.C.

600 UNIVERSITY STREET, SUITE 1012
SEATTLE, WASHINGTON 98101 USA
PHONE 206-632-7370, FAX 206-632-7487

1819 L STREET NW, NINTH FLOOR
WASHINGTON, D.C. 20036 USA
PHONE 202-347-9767, FAX 202-347-9766

NBR@NBR.ORG, WWW.NBR.ORG