FEATURE

Strategic Competition and Future Conflicts in the Indo-Pacific Region

Michael Raska

In the mid-twenty-first century, the Indo-Pacific's security hinges on the convergence of four major interrelated developments: (1) the adroit management of China's rise, both internal and external; (2) the challenge in reassessing strategic interests in the US-led web of Asian alliances; (3) the regional disparities in addressing endemic global security issues; and (4) the prevalence of traditional security quandaries in flashpoints such as the Taiwan Strait or the Korean Peninsula.[1] These trends are reflected in the struggle for dominance by the region's two major powers—China and Japan; the future of the Korean Peninsula; intraregional competition in territorial disputes in the East China Sea and South China Sea; and perhaps most importantly, the contours of long-term regional strategic competition and cooperation between China and the United States. At the same time, however, the Indo-Pacific security dynamics are bound to interlocking global and regional economic interdependencies, which present a paradox: notwithstanding historical rivalries and tensions, perennial strategic distrust, and weak multilateral regional institutional architecture, the Indo-Pacific's security complex is defined also by nonmilitary norms of state behavior.[2] These centripetal and centrifugal forces both amplify and mitigate sources of conflict in the region. Yet, the risks of miscalculation and potential confrontation exist: economic interdependencies cannot resolve the region's enduring security dilemmas amid contending national interests, strategies, and rising power-projection aspirations and capabilities. Seen from this perspective, this article argues that the increasing global and regional economic interdependencies juxtaposed by the strategic uncertainties, costs and risks of potential conventional conflicts shape preferences for long-term competitive strategies between major powers in the region. Consequently, asymmetric negation and strategic ambiguity in emerging new domains of warfare—space, cyberspace, near-space, and underwater—will increasingly characterize future conflicts in the Indo-Pacific.

To begin with, in every major security issue facing the Indo-Pacific, there is a major Chinese footprint, whether direct or indirect. The economic, political, and

military rise of China, reflected in three decades of relentless Chinese economic growth, has provided Beijing with new geopolitical opportunities by increasing the range of its strategic options and choices. At the same time, however, the attendant consequences of China's rise and its power-projection capabilities have led to perennial uncertainties surrounding its long-term political transition, and by extension, the Indo-Pacific's future security trajectories. As Zhu Feng noted, "China's greatest challenge is to manage its own rise—to take advantage of its stronger capabilities to expand its regional influence without provoking the regional instability that could undermine its long-term economic prosperity and integration."[3] Indeed, on one hand, China faces perennial internal political, socioeconomic, and environmental challenges that permeate into external foreign policy insecurities about its sovereignty, territorial integrity, and extended "core" national interests. On the other hand, China is seeking greatpower status—reasserting its geopolitical role and influence in the region by leveraging its global economic power and advancing military capabilities. The cumulative effects of these developments have been substantial as the People's Liberation Army's (PLA) catalogue of air, land, and naval platforms and assets are gradually catching up in terms of both qualitative sophistication and operational effectiveness.[4]

China's cumulative political, economic, and military rise is thus reshaping global and regional geopolitics, including the balance of power in the Indo-Pacific, in ways that are inherently detrimental for US interests and Washington's regional strategic partners and allies. Indeed, for nearly seven decades, the US strategy in the Asia-Pacific has remained relatively constant—maintaining robust forward active presence embedded in bilateral alliances to preserve access and mobility in the Western Pacific, and in doing so, defend its allies and ensure peace, stability, and prosperity in the region. While the United States continues to maintain comprehensive strategic advantages through its ongoing regional presence and relative military-technological superiority, China is arguably challenging Washington's ability to underwrite stability in the Indo-Pacific region.[5] In one school of thought, the diffusion of advanced military technologies coupled with asymmetric operational concepts is increasingly undermining US military advantages and, to a limited degree, its freedom of action in the region. Accordingly, the key issue for the US military is overcoming challenges of securing operational access in contested areas of global commons, and maintaining sufficient freedom of action—the ability to gain and maintain localized air superiority, maritime superiority, space and cyberspace superiority and security—in addition to the ability to conduct cross-domain operations and operational maneuver.[6]

These trends can be observed in China's aim for deeper regional power-projection into its "three seas" (the Yellow, East China, and South China Seas) or an area defined by the "first island chain," consisting of the Kuril Islands, Japan, Taiwan, and the South China Sea. Such projection is interpreted in US strategic thought as denying American forces freedom of action by restricting deployments of US forces into theater (antiaccess) and denying the freedom of movement of US forces already there (area denial).[7] Over the long term, however, China envisions its strategic control over its periphery up to the "second island chain," which means the dilution of US power up to American bases on Guam. The United States, meanwhile, with its policy of strategic rebalancing toward the Indo-Pacific, seeks to remain a "Pacific Power" through economic, diplomatic, cultural, and military presence and influence.[8]

Perhaps more importantly, deepening economic regional interdependencies and linkages juxtapose the strategic ramifications of the Sino-American contending visions, strategies, and interests, which poses complex challenges for traditional US alliance partners. Japan, South Korea, Australia, and ASEAN economies now trade more with China than with the United States. The chief challenge for these key regional US allies is pursuing two fundamentally opposing policy objectives: strengthening and maintaining security ties with the United States, while deepening economic linkages with China.[9] With the prevailing uncertainty about the future strategic and security landscape, US allies in the region—Japan, South Korea, and, to a lesser degree, Taiwan—are increasing their military spending and pursuing hedging strategies to address their expanding security concerns. Indeed, they are acquiring select indigenous power-projection capabilities, including reduced-signature fifth-generation air platforms; standoff precision weapons; ballistic and cruise missiles; early warning, intelligence, surveillance, and reconnaissance (ISR) assets as well as naval assets, including maritime patrol, antisubmarine warfare, and submarines.

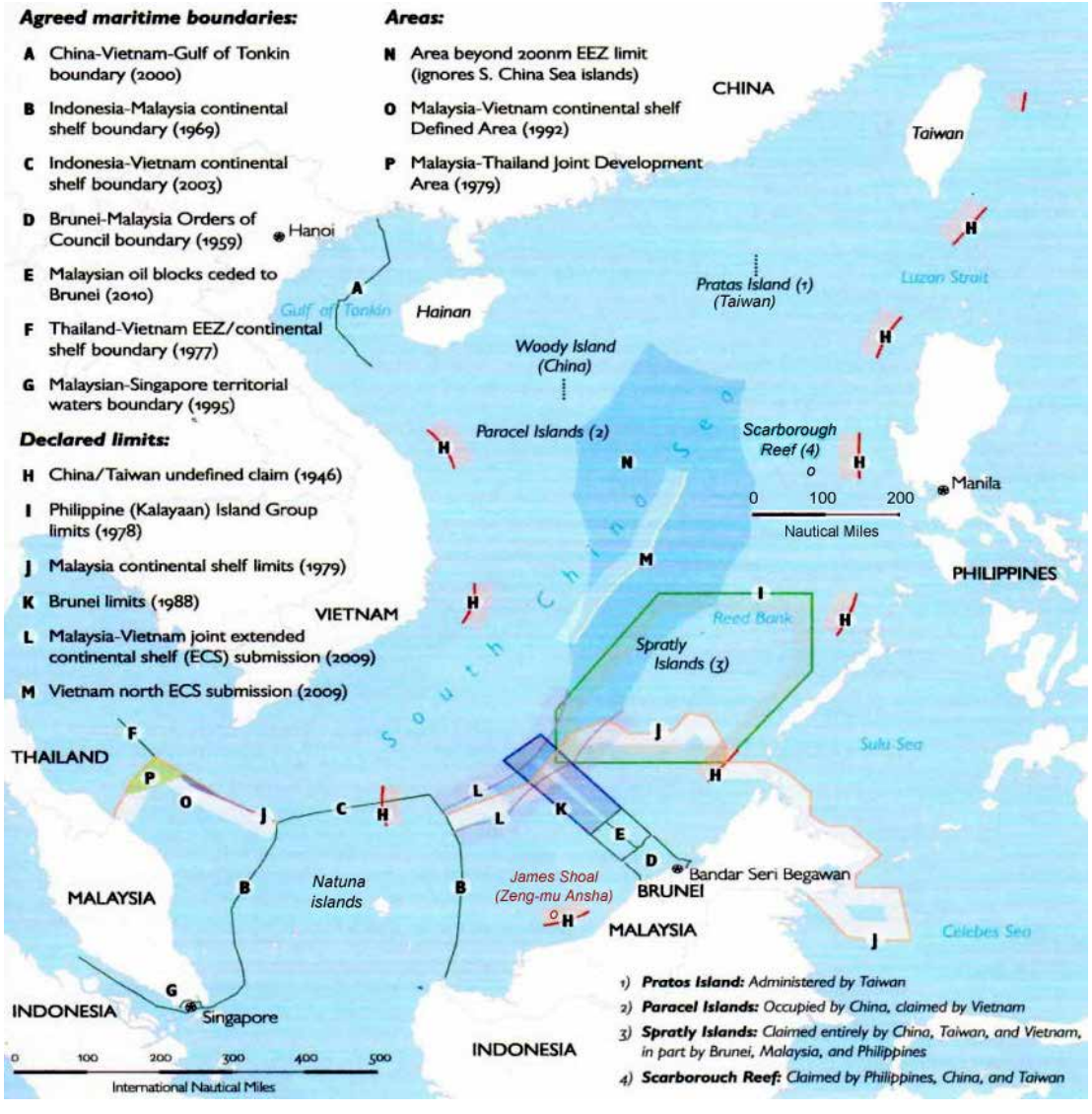

Figure 1. Sovereignty claims in the South China Sea. (Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* [Washington, DC: DOD, 2012], 37.).

At the same time, they are demonstrating the political willingness to use these assets for different strategic reasons. Japan seeks to overcome the limitations posed by its pacifist postwar constitution and the Yoshida Doctrine to exercise greater strategic adaptability and operational flexibility in responding to regional

contingencies, particularly North Korean ballistic missile threats and Sino-Japanese tensions in territorial disputes over the Senkaku/Diayou Islands in the East China Seas. In doing so, Tokyo is rethinking its national defense posture and its overall future security role in the region. In November 2013, Japan's cabinet under Prime Minister Shinzo Abe launched the country's first National Security Council, followed by the approval of the first National Security Strategy and increased efforts to reinterpret Japan's constitution.[10] South Korea's ongoing defense reforms and acquisition programs have aimed not only at strengthening capabilities vis-à-vis North Korean asymmetric threats but also developing joint air and naval capabilities that would complement long-term US strategic interests in the Indo-Pacific.[11]

Notwithstanding these strategic uncertainties, US allies in the region must also grapple with the operational consequences of Sino-US ongoing military-technological advances. In particular, as Carnes Lord and Andrew Erickson argue, the current constellation of US forward bases in the Indo-Pacific—including "main operating bases" with permanent US military presence, "forward operating sites" maintained by a relatively small US support presence for temporary deployments, and "cooperative security locations" designed for contingency use with little or no permanent US presence—will become increasingly vital, yet paradoxically vulnerable" with the emergence of robust Chinese theater-strike capabilities.[12] At the same time, US allies in the Indo-Pacific must calculate their potential future roles, level of active participation, and defense resource allocation requirements supporting future US military strategy and operational conduct in the region—envisioned in concepts such as the Joint Concept for Access and Maneuver in the Global Commons (JAM-GC) formerly known as AirSea Battle.[13]

Smaller- and medium-sized states in Southeast Asia are also gradually modernizing their naval and air forces to keep their vital sea lanes open, conduct intelligence missions, and, perhaps most importantly, provide options for deterring China's naval forces from seizing disputed islands in the South China Sea. While there are different political, strategic, and technological drivers shaping regional military modernization trajectories, including long-standing intraregional rivalries and competition over borders, resources, and history, most Southeast Asian countries share concerns about China's "coercive diplomacy," military capabilities, and future aspirations in the region.

Consequently, Southeast Asian countries are responding by revamping their force modernization priorities, partnerships, and overall strategic choices. Given their varying levels of development and defense resource allocation, however, their military-technological trajectories show considerable variation in the pace, direction, scope, and character of adaptation. This is reflected in the resulting regional

"arms competition," characterized by incremental, often near-continuous, improvements of existing capabilities as well as in a mix of cooperative and competitive pressures; continued purchases of advanced weapon platforms, including the introduction of new types of arms; and therefore, unprecedented military capabilities.[14] In short, China's increasing power-projection capabilities are gradually redefining regional military balance and, subsequently, US strategy and that of its partners and allies. The resulting broader strategic debates converge on the question of how to attain long-term, credible, cross-domain, attack-and-defense in-depth capabilities while sustaining joint operational capabilities in select contested areas in the Indo-Pacific and simultaneously mitigating a range of escalatory risks.

China's Military Modernization

In the context of the above strategic debates is the challenge of ascertaining the pace, character, direction, magnitude, and impact of China's ongoing military modernization. Indeed, China's development of its military capabilities under Pres. Xi Jingping has seen many accomplishments—from the introduction of the next generation of supercomputers to aviation prototypes such as the J-16, J-20, J-31; from new helicopters and UAVs to the ongoing construction of a second aircraft carrier; and a record number of commissioned ships such as Type 054A, 056 frigates, and 052C destroyers. Arguably, China's political and military elites believe that a new wave of the global revolution in military affairs is gathering pace, led principally by the United States, and Beijing must therefore accelerate the pace of its military development. In the next 5–10 years, China is expected to transfer many experimental models from a research-and-development (R&D) phase to a production stage, including a number of systems in what the PLA calls domains of emerging "military rivalry": outer space, near-space, cyberspace, and underwater.[15] These include the next generation of ballistic missiles, nuclear and conventional, long-range precision-strike assets such as hypersonic vehicles, offensive and defensive cyber-capabilities, new classes of submarines, supported by a variety of high-tech, directional rocket rising sea mines with accurate control-and-guidance capacity. The key question, however, is whether China's defense industries and the PLA can sustain their relative progress in terms of confronting internal constraints while facing external competition?

Photo courtesy of Danny Yu,
http://www.airliners.net/photo/China-Air-Force/Shenyang-J-31-F60/2546527/L.

Figure 2. Shenyang FC-31 (F60) at 2014 Zhuhai Air Show.

Since the late 1990s, the PLA has been selectively upgrading its existing weapons systems and platforms, while experimenting with the next generation of design concepts. This is apparent in the gradual modernization of China's nuclear and conventional ballistic missiles; integrated air, missile, and early warning defense systems; electronic and cyberwarfare capabilities; submarines; surface combat vessels; and fourth- and fifth-generation multirole combat aircraft.[16] With the qualitative shifts in "hardware," the PLA has been also revamping its "software"—military doctrine, organizational force structure, operational concepts, and training. Notwithstanding the PLA's most important grand strategic objective—the preservation of the political supremacy of the Chinese Communist Party (CCP)—embedded in the concept of "safeguarding China's national sovereignty, national security, and territorial integrity and supporting China's peaceful development," the scope of its "core missions" has been gradually extending. The PLA's mission templates now include both "traditional" as well as "new" missions consistent with

the objective of protecting China's national sovereignty, security, and territorial integrity.[17]

According to a recent study, the PLA's notion of traditional missions includes Beijing's traditional threat perceptions that have remained relatively constant since the founding of the PRC in 1949: "resisting aggression" from neighboring countries, such as India and Russia, and countries that can project power into China's territorial and maritime domains, such as the United States. Additionally, this notion includes "containing separatist forces" in the provinces of Xinjiang and Tibet and deterring Taiwan moves toward independence. Furthermore, the concept includes "safeguarding border, coastal, and territorial air security" from intervention or interference from either state or non-state threats. Moreover, the PLA has increasingly placed an emphasis on "protecting national security interests in space and cyberspace" as a core mission-domain.[18]

At the same time, the PLA has been gradually expanding its area of operations under the broader concept of "New Historic Missions," in line with "China's peaceful development" strategy that essentially provides legitimacy for the CCP. The new missions include "participating in emergency rescue and disaster relief operations," internally and externally; "subduing subversive and sabotage attempts and cracking down on separatist forces" to counter terrorism; "accomplishing security provision and guarding tasks" through the PLA's involvement in peacekeeping operations; "merchant vessel protection" for state and non-state actors; "evacuation of Chinese nationals overseas"; and "security support for China's interests overseas," including protecting maritime commerce through antipiracy operations.[19]

The shifting character of the PLA's operational template toward diversified missions in turn compels the Chinese defense industry to deliver much-more-advanced weapons platforms, system, and technologies. For most of its history, however, the results of these endeavors have been decidedly mixed. According to Richard Bitzinger et.al., as late as the late 1990s, China still possessed one of the most technologically backward defense industries in the world; most indigenously developed weapons systems were at least 15 to 20 years behind those of the West—basically comparable to 1970s- or (at best) early 1980s-era technology—and quality control was consistently poor. Observers generally regarded China's defense R&D base to be deficient in several critical areas, including aeronautics, propulsion (such as jet engines), microelectronics, computers, avionics, sensors and seekers, electronic warfare, and advanced materials.[20] Furthermore, the Chinese military-industrial complex was traditionally weak in the area of systems integration—that is, the ability to design and develop a piece of military equipment that integrates hundreds or even thousands of disparate components and

subsystems. Consequently, aside from a few "pockets of excellence" such as ballistic missiles, the Chinese military-industrial complex appeared to demonstrate few capacities for designing and producing relatively advanced conventional weapons systems. Especially when it came to combat aircraft, surface combatants, and ground equipment, the Chinese generally confronted considerable difficulties when it came to moving prototypes into production, resulting in long development phases, heavy program delays, and low production runs.[21]

Historically, the development of China's defense industry progressed gradually in four overlapping waves: (1) the Maoist Era (1949–1978), (2) Deng's Demilitarization Era (1980s–1990s); (3) Reform Era (1998–2012); and (4) the current Xi Jingping's Reform Era 2.0 (2012–present).[22] In 2003, after another decade of stagnation, Beijing decided to build a new civilian technological and industrial base with embedded military capabilities (Yujun Yumin). At that time, China's political establishment envisioned this strategy as paving the way for a new round of associated reforms in the defense industry, including allowing select private-sector firms to engage in defense work. The key areas of China's dual-use technology development and subsequent spin-on included microelectronics, space systems, new materials (such as composites and alloys), propulsion, missiles, computer-aided manufacturing, and particularly information technologies. Subsequently, Yujun Yumin became a priority in the last several Five-Year Defense Plans. These plans have emphasized the importance of the transfer of commercial technologies to military use, calling upon the Chinese arms industry to not only develop dual-use technologies but also to actively promote joint civil-military technology cooperation. In the early 2000s, Beijing worked hard to encourage further domestic development and growth in these sectors and to expand linkages and collaboration between China's military-industrial complex and civilian high-technology sectors.[23]

Currently, China's long-term strategic military programs yield evidence of deep integration with China's advancing civilian science and technology (S&T) base, which in turn is increasingly linked to global commercial and scientific networks. Technology transfers, foreign R&D investment, and training of Chinese scientists and engineers at research institutes and corporations overseas are part of China's indigenous innovation drive to identify, digest, absorb, and reinvent (IDAR) select technological capabilities, in civil and military domains.[24] In the process, Beijing is benchmarking emerging technologies and similar high-tech defense-related programs in the United States, Russia, India, Japan, Israel, and other countries.[25] Specifically, China's government under President Xi views the indigenous innovation strategy as mutually supporting the PLA's military modernization and the country's economic future to achieve long-term sustainable

growth, efficiency, and productivity gains, while mitigating serious problems, including labor shortages, stretched resource supplies, unequal distribution of income, social tensions, and unprecedented environmental pollution. In the process, China is attempting to translate its absorptive capacity to recognize, assimilate, and utilize new and external knowledge into an innovative capacity that may in theory lead to disruptive innovation. Inherently, IDAR also aims to circumvent the costs of research, overcome technological disadvantages, and leapfrog China's defense industry by leveraging the creativity of other nations. This includes exploitation of open sources, technology transfer and joint research, the return of Western-trained Chinese students, and, of course, industrial espionage—both traditional and, increasingly, cyberespionage.[26]

Notwithstanding the much-improved technological capabilities, however, the potential of Chinese defense S&T is still constrained in its continuing path dependencies. These include overlapping planning structures, widespread corruption, bureaucratic fragmentation, and most importantly, no real internal competition. Other barriers to innovation also include ensuring the structural strength, quality control, process standardization, evident for example in the development of engines required for next-generation aircraft. In the long term, the question is whether China will transform into a leading critical technological innovator of major weapons platforms and systems comparable in sophistication to global defense S&T powers. China's historical path dependence suggests this is unlikely. However, China will continue to seek niche technological developments that could potentially revolutionize the PLA's military operations by providing a credible asymmetric edge in regional flashpoints: i.e., anti-ship ballistic missiles, anti-satellite ballistic missiles, hypersonic cruise missiles, and systems converging cyber and space capabilities. Ultimately, as China becomes more technologically advanced, Beijing's ability to align its strategic goals with technological advancements will increasingly shape its military effectiveness. These, however, must be viewed in the relative and comparative context of other countries' technological developments.[27]

Cyber-Enabled Future Conflict Trajectories

With the convergence of conventional, asymmetric, low-intensity, and nonlinear security threats—coupled with the diffusion of advanced military and dual-use technologies—one could argue that the Indo-Pacific's future conflict spectrum will be increasingly characterized through overlapping strategic rivalries in multiple domains: space, cyberspace, near-space, underwater, and information. These domains enable and reinforce strategic ambiguity in terms of effects, sources, and motives.[28] For example, nearly all cyber-operations are based on the

use of ambiguity—neither confirming nor denying direct use of cyber-weapons vis-à-vis existing or potential adversaries and their select proxy targets. Direct and, to a lesser degree, indirect results of cyberwarfare are often invisible, which amplifies uncertainties on the sources of the intrusion, attack, or malfunction. Even if the source is known or detected, the purpose of the cyberattack might be less clear. Perpetrators may frame deliberate attacks to mislead people or their equipment. As Martin Libicki noted, "if cyber-attacks work—and this is a tremendous if—they change the risk profile of certain actions, and usually in ways that make them more attractive options."[29] Accordingly, cyber-strategies may be used as a response to a limited kinetic attack or aggression with a lesser risk of escalation than a physical retaliation. Alternatively, cyber-strategies can be used to affect the outcome of a conflict in another state without any visible commitments. Consequently, however, strategic ambiguity may shape the propensity for offensive cyber-operations given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence.[30]

The convergence of the above characteristics of cyberspace as a warfighting domain translates into a continuously expanding tactical envelope for cyber-kinetic operations, and perhaps more importantly, increasing strategic overlap with other domains of warfare—physical, informational, and cognitive. In the former, the concept of *cyberspace*—broadly characterized as a virtual information environment supported by system-of-systems physical infrastructures—increasingly serves as a mutually supporting layer connecting, empowering, and enabling content, actions, and capabilities of land, sea, air, and space systems operating in all physical domains. Simultaneously, the use of cyberspace in the information domain is intended to use either for *exploitation*—how the use or manipulation of information can be utilized to an advantage—or *protection*—how to prevent an opponent from using or manipulating information to an advantage. Moreover, cyberspace is also increasingly used as a sphere of influence in the psychological or cognitive domain—in the ability to penetrate target audiences in real time, for example, crafting messaging campaigns to go "viral" to create cognitive effects, whether cohesive or divisive. Accordingly, traditional regional security flashpoints in the East and South China Seas, the Korean Peninsula, and the Taiwan Straits will likely have parallel and continuous confrontations in and out of cyberspace, with potential cyberattacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyberespionage.

In China, the PLA's Strategic Support Force has conceptualized future conflicts under the construct of integrated network electronic warfare (网电一体战 wangdian yitizhan, or INEW). INEW's principles closely emulate Russian

conceptions through a holistic representation that combines simultaneous and coordinated use of computer network operations (CNO), electronic warfare, and kinetic strikes designed to paralyze an enemy's networked information systems. These include the PLA's electronic warfare and counter space forces using electronic jamming, electronic deception, and suppression to disrupt information acquisition and information transfer; and the PLA's computer network attack and exploitation units to disrupt, destroy, or subvert an adversary's data and networks using advanced virus attacks, hacking, deception, and sabotage information processing. INEW is expected to be employed in the earliest phases of a conflict and possibly preemptively with the objective to deny the enemy access to information essential for continued combat operations by creating "blind spots" against an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems.[31]

For the PLA, achieving information dominance (制信息权 zhi xinxi quan) is a key prerequisite for allowing the PLA to seize air and naval superiority, according to two of the PLA's most authoritative public statements on its doctrine for military operations: "The Science of Military Strategy" and "The Science of Campaigns." Both documents identify an enemy's C4ISR and logistics systems networks as the highest priority for select INEW operations. At the same time, the PLA recognizes the importance of controlling space-based information assets as a means of achieving true information dominance, calling it the "new strategic high ground." Meanwhile, the PLA's cyber units are involved in comprehensive cyber reconnaissance, probing the computer networks of foreign government agencies and private companies. These activities, which China denies, serve to identify weak points in networks, understand how foreign leaders think, discover military-communication patterns, and attain valuable technical information stored throughout global networks.

Consequently, the effectiveness of conventional defense strategies and weapons technologies could be potentially negated through a range of CNOs—defensive, offensive, and intelligence-driven, such as exploiting vulnerabilities in the country's systems and technologies for C4ISR.[32] For militaries, cyber-enabled conflicts will evolve parallel with technological changes (i.e., the introduction of next-generation robots and remotely controlled systems) that will alter the character of future warfare. Cyberspace and space are likely to become major theaters of operations, arenas of continuous struggle, as major regional powers will continue to invest in full-spectrum CNO capabilities. The key challenge for militaries in the Indo-Pacific will center on ensuring the security, reliability, and integrity of country's mission-critical C4ISR systems that will become increasingly vulnerable to cyber threats as well as other emerging forms of electronic warfare, including

threats from electromagnetic pulse and high-powered microwave weapons. The propensity for cyber-offensive operations will create a greater uncertainty about the functionality of C4ISR in the event of a regional crisis.[33]

Inherently, these challenges will apply to nearly all operational functions and processes that depend to some extent on cyberspace, including combat support and logistics systems. A sophisticated cyberattack on these systems would likely result in cascading effects with ramifications for the individual services and their abilities to carry out operational missions. Depending on the magnitude of cyberattacks on combat support systems, the operational capabilities will likely degrade. If the effects are immediate, the system degrades catastrophically. If the effects are gradual, the system's functions will degrade in phases depending on the ability to identify, diagnose, respond, and recover from the attack. Therefore, military organizations will have to focus on achieving operational mission assurance rather than traditional information assurance. A number of factors, including vulnerability and impact assessment of combat and logistics support systems that fall into a high criticality/high risk areas to operational missions will determine the ability to respond and recover from a major cyberattack.[34]

Conclusion

In the long term, the deepening socioeconomic interdependencies and information architectures integrated in nearly all aspects of civilian governance (i.e., energy systems, communications, water, transportation, finance, and so forth) could be compromised to varying levels through various cyber-enabled operations. Consequently, the continuously evolving character and reliance on cyberspace in civil-military domains provides a new arena for strategic competition, increases uncertainty, and enables a spectrum of operations other than war.

With the widening complex operational requirements, the United States and its partners and allies may have to rethink existing concepts of operations, doctrinal command-and-control methodologies, organizational force structures, training programs, and ultimately, military-technological acquisition priorities. Indeed, major changes in the direction and character of conflicts will have implications on defense planning, resource allocation, training, organization and the use of force—propelling the need for a sustained conceptual, organizational, and technological innovation intended to enhance the military's ability to prepare for, fight, and win new types of wars. In this context, US strategic partners and allies in the Indo-Pacific must enhance their ability to change military posture rapidly based on the changes in geostrategic environment, while having the flexibility and robustness to employ novel strategies, tactics, and technologies in different ways and scenarios. As new strategic realities create new powers, new types of future conflicts

will emerge. Select military technologies and capabilities will diffuse to other major and many minor military powers, reshaping the paths and patterns of regional military modernization. The confluence of new strategies, technologies, organizations, and doctrines in the broader context of global power transitions will shape the direction, pace, character, and outcome of military change in the Indo-Pacific. JIPA

Notes

1. Chung-Min Lee and T. J. Pempel, "The Northeast Asian Security Complex: History, Power, and Strategic Choices," in *Security Cooperation in Northeast Asia: Architecture and Beyond*, ed. Chung-Min Lee and T. J. Pempel (New York: Routledge, 2012), 3–21.
2. T. J. Pempel, "Security Architecture in Northeast Asia: Projections from the Rearview Mirror," in *Security Cooperation in Northeast Asia: Architecture and Beyond*, ed. Chung-Min Lee and T. J. Pempel (New York: Routledge, 2012), 212–32.
3. Zhu Feng, "An Emerging Trend in East Asia: Military Budget Increases and Their Impact," *Asian Perspective* 33, no. 4, (2009): 17–45.
4. Andrew Erickson, "China's Modernization of its Naval and Air Power Capabilities," in *Strategic Asia 2012-13: China's Military Challenge*, ed. Ashley Tellis and Travis Tanner (Washington, DC: National Bureau of Asian Research, 2012), 60–125.
5. Dan Blumenthal, "The Power Projection Balance in Asia," in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas Mahnken (Stanford, CA: Stanford University Press, 2012), 168.
6. Terry Morris, et al., "Securing Operational Access: Evolving the Air-Sea Battle Concept," *National Interest*, March/April (2015), 69–73.
7. Benjamin Schreer, *Planning the Unthinkable War: AirSea Battle and its Implications for Australia*, Australian Strategic Policy Institute Monograph (Barton, Australia: Australian Strategic Policy Institute, April 2013), 8.
8. Ely Ratner, "Rebalancing to Asia with an Insecure China," *Washington Quarterly* 36, no. 2 (2013): 21–38.
9. Lee and Pempel, "The Northeast Asian Security Complex," 4.
10. James Hardy, "Strong Constitution: Japan Looks to Reset its Policy on Self-Defence," *IHS Jane's Intelligence Review*, 14 May 2014.
11. Chung Min Lee, "East Asia's Awakening from Strategic Hibernation and the Role of Air Power," *Korean Journal of Defense Analysis* 15, no. 1 (2003): .219–74.
12. Carnes Lord and Andrew Erickson, "Guam and American Security in the Pacific," in *Rebalancing U.S. Forces: Basing and Forward Presence in the Asia-Pacific*, ed. Carnes Lord and Andrew Erickson (Annapolis, MD: Naval Institute Press, 2014), 9.
13. Richard Bitzinger and Michael Raska, "The AirSea Battle Debate and the Future of Conflict in East Asia," *RSIS Policy Brief* (2013), 6.
14. Richard Bitzinger, "A New Arms Race? Explaining Recent Southeast Asian Military Acquisitions," *Contemporary Southeast Asia* 32, no. 1 (2010): 50–69.
15. Tai Ming Cheung, "Introduction," in *Forging China's Military Might: A New Framework for Assessing Innovation,* ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2014), 1–15.
16. Anthony Cordesman, Ashley Hess, and Nicholas Yarosh, *Chinese Military Modernization and Force Development*, (Washington, DC: Center for Strategic and International Studies, 2013).
17. Michael Chase, et al., *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army* (Santa Monica, CA: RAND Corporation, 2015), 26.
18. Ibid.

19. Ibid.
20. Richard Bitzinger, et al., "Locating China's Place in Global Defense Economy," in *Forging China's Military Might: A New Framework for Assessing Innovation*, ed. Tai Ming Cheung (Baltimore, MD: Johns Hopkins University Press, 2014), 171.
21. Evan S. Medeiros, et al., *A New Direction for China's Defense Industry* (Santa Monica, CA: RAND, 2005), 4–18.
22. Tai Ming Cheung, *Fortifying China: The Struggle to Build a Modern Defense Economy* (Ithaca, NY: Cornell University Press, 2009).
23. Ibid.
24. Tai Ming Cheung, "The Chinese Defense Economy's Long March from Imitation to Innovation," *Journal of Strategic Studies* 34, no. 31 (2011): 325–54.
25. DOD Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013).
26. Jon Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon Lindsay, Tai Ming Cheung, and Derek Reveron (New York: Oxford University Press, 2015), 66.
27. Richard Bitzinger and Michael Raska, "Capacity for Innovation: Technological Drivers of China's Future Military Modernization," in *The Chinese People's Liberation Army in 2025*, ed. Roy Kamphausen and David Lai (Carlisle, PA: US Army War College Press, 2015), 129–62.
28. Martin Libicki, "The Strategic Uses of Ambiguity in Cyberspace," *Military and Strategic Affairs* 3, no. 3 (2011): 3–10.
29. Ibid., 6.
30. Lior Tabansky, "Basic Concepts of Cyberwarfare," *Military and Strategic Affairs* 3, no. 3 (2011): 75–92.
31. Michael Raska, "Revealed: The New Battleground in China's Future Wars," *National Interest*, 10 March 2015, https://nationalinterest.org/feature/revealed-the-battleground-chinas-next-war-12387.
32. Paul Davis and Peter Wilson, *Looming Discontinuities in U.S. Military Strategy and Defense Planning*, RAND Occasional Papers 326 (Santa Monica, CA: RAND, 2011), 12.
33. Ibid.
34. Don Snyder, et al., *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems*, RAND Research Report RR620 (Santa Monica, CA: RAND, 2015).

Dr. Michael Raska
Michael Raska is an assistant professor at the Institute of Defense and Strategic Studies, based at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.