Strategic Transformation and Military Modernization in the Asia-Pacific Region

Michael Raska, Ph.D.
Research Fellow
Military Transformations Program
Institute of Defense and Strategic Studies
S. Rajaratnam School of International Studies
Nanyang Technological University
ismraska@ntu.edu.sg
Abstract:

As new strategic realities create new powers, new types of future conflicts emerge. In the early 21st century, East Asia’s security is shaped by contending trajectories, including the pace, character, and direction of China’s military modernization; the struggle for dominance by the region’s two major powers (China and Japan); the future of the Korean Peninsula; intra-regional 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 rivalry between China and the United States. These are amplified by perennial strategic distrust among major regional powers, as well as by ongoing diffusion and integration of advanced military technologies in nearly every combat domain. At the same time, however, East Asian security dynamics is bound to interlocking global and regional economic interdependencies, which present a paradox: notwithstanding historical rivalries and tensions, perennial strategic distrust, weak multilateral regional institutional architecture, East Asia’s security complex is defined also by non-military norms of state behavior. In this context, this paper 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, future conflicts in East Asia will be increasingly characterized by the combination of asymmetric negation, strategic ambiguity, denial and deception particularly in the emerging new domains of warfare: space, cyberspace, near-space, and underwater. These will evolve into state-led ‘hybrid conflicts’ characterized by a convergence of ‘cyber-kinetic-information conflicts’ and their strategic interactions.

About the Author:

Michael Raska is a Research Fellow at the Institute of Defense and Strategic Studies, based at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

Note:
For questions, comments, suggestions please contact the authors: ismraska@ntu.edu.sg
East Asia’s Complex Security Environment

In the early 21st century, East Asia’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 U.S.-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. 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; intra-regional 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, East Asian security dynamics is bound to interlocking global and regional economic interdependencies, which present a paradox: notwithstanding historical rivalries and tensions, perennial strategic distrust, weak multilateral regional institutional architecture, East Asia’s security complex is defined also by non-military norms of state behavior. 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 paper 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, future conflicts in East Asia will be increasingly characterized by asymmetric negation and strategic ambiguity in emerging new domains of warfare: space, cyberspace, near-space, and underwater.

To begin with, in every major security issue facing East Asia, there is a major Chinese footprint, both direct and 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, East Asia’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.” Indeed, on one hand, China faces perennial internal political, socio-economic, 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 great-power status - reasserting its geopolitical role and influence in the region by leveraging its global economic power and advancing military capabilities. In 2014, China spent US$131 billion on its defense budget, up 12.2 percent from the 2013 budget estimated at US$119 billion – marking 17 straight years of near-double digit increases in defense spending. The cumulative effects of these developments have been substantial as the PLA’s catalogue of air, land, and naval platforms and assets are gradually catching-up in terms of both qualitative sophistication and operational effectiveness.

---

China’s cumulative political, economic, and military rise is thus reshaping global as well as regional geopolitics, including the balance of power in East Asia in ways that are inherently detrimental for the U.S. interests and its regional strategic partners and allies. Indeed, for nearly seven decades, the U.S. 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 U.S. continues to maintain comprehensive strategic advantages through its continuing regional presence and relative military-technological superiority, its ability to underwrite stability in the Asia Pacific region is arguably challenged by China. In one school of thought, the diffusion of advanced military technologies coupled with asymmetric operational concepts are increasingly undermining U.S. military advantages and, to a limited degree, its freedom of action in the region. Accordingly, the key issue for the U.S. 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. 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 is interpreted in the U.S. strategic thought as denying U.S. forces the freedom of action by restricting deployments of U.S. forces into theatre (anti-access) and denying the freedom of movement of U.S. forces already there (area denial). Over the long-term, however, China envisions its strategic control over its periphery up to the ‘second island chain’, which means the dilution of U.S. power up to its bases on Guam. The United States, meanwhile, with its policy of Strategic Rebalancing toward the Asia-Pacific, seeks to remain a “Pacific Power” through economic, diplomatic, cultural, and military presence and influence.

Perhaps more importantly, the strategic ramifications of the Sino-American contending visions, strategies, and interests are juxtaposed by deepening economic regional interdependencies and linkages, which poses complex challenges for traditional U.S. alliance partners. Japan, South Korea, Australia, as well as ASEAN economies now trade more with China than the United States. The key challenge for these key regional U.S. allies is pursuing two fundamentally opposing policy objectives: strengthening and maintaining security ties with the United States, while deepening economic linkages with China. With the prevailing uncertainty about the future strategic and security landscape, U.S. 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 assets as well as naval assets, including maritime patrol, anti-submarine warfare, and submarines. 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/Diaoyou 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 pacifist constitution.\(^\text{11}\) 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 U.S. strategic interests in East Asia.\(^\text{12}\) Notwithstanding these strategic uncertainties, U.S. allies in the region must also grapple with operational consequences of Sino-U.S. ongoing military-technological advances. In particular, as Carnes Lord and Andrew Erickson argue, the current constellation of U.S. forward bases in East Asia: “main operating bases” with permanent U.S. military presence, “forward operating sites” maintained by a relatively small U.S. support presence for temporary deployments, and “cooperative security locations” designed for contingency use with little or no permanent U.S. presence will become increasingly vital, yet paradoxically vulnerable\(^{13}\) with the emergence of robust Chinese theater-strike capabilities.\(^{13}\) At the same time, U.S. allies in Northeast Asia must calculate their potential future roles, the level of active participation, and defense resource allocation requirements supporting future U.S. 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.\(^\text{14}\)

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 of 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 their 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.\(^\text{15}\) In short, China’s increasing power-projection capabilities are gradually redefining regional military balance and subsequently U.S. strategy and that of its partners and allies. The resulting broader strategic debates converge on the question 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 Asia-Pacific, and simultaneously mitigating a range of escalatory risks.

Debating 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 President Xi Jingping has seen many accomplishments: from the introduction of next generation of supercomputers, to aviation prototypes such as the J-16, J-20, J-31, new helicopters, UAVs, to the ongoing construction of a second aircraft carrier, as well as 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 U.S, and China must therefore accelerate the pace of its military development. In the next 5-10 years, China is expected to transfer many experimental models from an R&D to a production stage, including a number of systems in what the PLA calls - domains of emerging “military rivalry”: outer space, near space, cyber space & under water. These include 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 as well as the PLA can sustain their relative progress both in terms of confronting its internal constraints, while facing external competition?

Since the late 1990’s, the PLA has been selectively upgrading its existing weapons systems and platforms, while experimenting with the next generation of design concepts. These can be seen 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 the introduction of fourth/fifth generation of multi-role combat aircraft. 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 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. According to one group of analysts, the former includes Beijing’s traditional threat perceptions that have remained relatively constant since the founding of the PRC in 1949: “resisting aggression” from both neighboring countries, such as India and Russia (formerly the Soviet Union), and countries that can project power into China’s territorial and maritime domains, such as the United States; “containing separatist forces” in the provinces of Xinjiang and Tibet and deterring Taiwan moves toward independence; and “safeguarding border, coastal, and territorial air security” from intervention or interference from either state or nonstate threats. Moreover, the PLA has increasingly placed an emphasis on “protecting national security interests in space and cyberspace” as a core mission-domain. 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” both 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

19 Ibid.
involvement in peacekeeping operations; “merchant vessel protection” for both state and non-state actors; “evacuation of Chinese nationals overseas”; and “security support for China’s interests overseas” including protecting maritime commerce through anti-piracy operations.\(^\text{20}\)

The shifting character of 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 backwards defense industries in the world; most indigenously developed weapons systems were at least 15 to 20 years behind that of the West – basically comparable to 1970s- or (at best) early 1980s-era technology – and quality control was consistently poor. China’s defense research and development (R&D) base was regarded 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.\(^\text{21}\) Furthermore, the Chinese military-industrial complex was traditionally been 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 weapon systems. Especially when it came to combat aircraft, surface combatants, and ground equipment, the Chinese generally confronted considerable difficulties when it comes to moving prototypes into production, resulting in long development phases, heavy program delays and low production runs.\(^\text{22}\)

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 current (4) Xi Jingping’s Reform Era 2.0 (2012-present).\(^\text{23}\) In 2003, after another decade of stagnation, a decision was made to build new civilian technological and industrial base with embedded military capabilities (Yujun Yumin). At that time, China’s political establishment envisioned this strategy as paving 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 not only to develop dual-use technologies, but also actively promote joint civil-military technology cooperation. In the early 2000s, Beijing has worked hard both 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.\(^\text{24}\)

Currently, China’s long-term strategic military programs yield evidence of deep integration with China’s advancing civilian science and technology 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 (1) identify, (2) digest, (3) absorb, and (4) reinvent select

\(^{20}\text{Ibid. p. 26.}\)


\(^{22}\text{Evan S. Medeiros, Roger Cliff, Keith Crane, and James C. Mulvenon, A New Direction for China’s Defense Industry (Santa Monica, CA: RAND, 2005), pp. 4-18.}\)

\(^{23}\text{Tai Ming Cheung, Fortifying China: The Struggle to Build a Modern Defense Economy (Ithaca, NY: Cornell University Press, 2009).}\)

\(^{24}\text{Ibid.}\)
technological capabilities, both in civil and military domains. In the process, China is benchmarking emerging technologies and similar high-tech defense-related programs in the United States, Russia, India, Japan, Israel and other countries. Specifically, China’s government under President Xi views “indigenous innovation” strategy as mutually supporting both PLA’s military modernization as well as the country’s economic future to achieve a 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 attempts to translate its absorptive capacity to recognize, assimilate, and utilize new and external knowledge into 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, cyber-espionage.

Notwithstanding the much improved technological capabilities, however, the potential of Chinese defense S&T is still constrained in its continuing path dependence. This includes 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 the 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 (ASBMs), anti-satellite ballistic missiles (ASBMs), hypersonic cruise missiles, and systems converging cyber and space capabilities. Ultimately, as China becomes more technologically advanced, its military effectiveness will be increasingly shaped by China’s ability to align its strategic goals with technological advancements. These, however, must be viewed in the relative and comparative context of other countries’ technological developments.

Paths and Patterns of East Asia’s Future Conflicts

With the convergence of conventional, asymmetric, low-intensity, and non-linear security threats; coupled with the diffusion of advanced military and dual-use technologies, one could argue that East Asia’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. 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 cyber warfare 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 cyber-attack might be less clear. Deliberate attacks may be framed 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.” 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 increase the propensity for offensive and unrestricted cyber operations given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence.

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, i.e. cohesive or divisive. Accordingly, traditional regional security flashpoints in the East and South China Seas, the Korean Peninsula, the Taiwan Straits will likely have parallel and continuous confrontations in and out of cyber space, with potential cyber-attacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage.

At the same time, however, cyberspace differs from existing strategic environments in terms of transcending traditional boundaries of geography and time. Consequently, it is important to distinguish between the different types of cyber-enabled conflicts applicable to East Asia: confrontations in cyberspace (similar to the 2007 attack on Estonia, attributed to Russia); conflicts in which cyberspace complements other components in the use of force (similar to Russia’s attack on Georgia in 2008). Furthermore, one can differentiate between different types of targets: attacks on computerized systems taking place in cyberspace; cyber-attacks targeting the physical domain (similar to the 2009 Stuxnet attack on Iran’s nuclear program). In each category, there are different forms of attacks such as denial, deception disruption, and subversion; as well as different levels of magnitude and impact – from stealth cyber-intelligence collection and military-cyber reconnaissance preparations, economic sabotage, to actual attacks with direct physical effects causing damage, disruption, or destruction of computerized systems or targets in the physical domain: actions with direct effects on a nation (such as industrial disruption).

---

30 Ibid. p. 6
31 As Lior Tabansky notes, the limited risk is a function of: the difficulty in distinguishing between a glitch and an attack; the difficulty in connecting an event with a result; the difficulty in tracking the source of the attack and identifying the attacker; widespread use of inexpensive, off the shelf technologies; and the many vulnerabilities of a computer system. The cyber threat is asymmetric: no great investment is required for developing and using the weapons. In contrast, defense against cyber threats must encompass all channels of attack and keep up to date with new developments, and the cost of defense continues to grow. See: Lior Tabansky, “Basic Concepts of Cyberwarfare,” Military and Strategic Affairs, vol. 3, no.3 (2011), p.75-92.
will have offline consequences, and vice-versa. The diffusion of select cyber capabilities, whether defensive or offensive, may not only augment traditional military capabilities of major powers in the region, but more importantly, provide a new set of strategic challenges as well as opportunities for the U.S. and its allies in the region.

In China, the PLA has conceptualized future conflicts under the *Integrated Network Electronic Warfare* (*wangdian yizhan*) or INEW. Its principles closely emulate Russian conceptions through a holistic representation that combines simultaneous and coordinated use of computer network operations (CNOs), electronic warfare (EW), and kinetic strikes designed to paralyze an enemy’s networked information systems. These include (1) the PLA’s Electronic Warfare and Counter-Space Forces using electronic jamming, electronic deception and suppression to disrupt information acquisition and information transfer; (2) 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 pre-emptively with the objective to deny the enemy access to information essential for continued combat operations by creating “blind spots” against an adversary’s C4ISR systems.  

For the PLA, achieving information dominance (*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, 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 computer network operations (CNOs) – defensive, offensive, and intelligence-driven, such as exploiting vulnerabilities in the country’s systems and technologies for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). For militaries, cyber-enabled conflicts will evolve parallel with technological changes (i.e. the introduction of next generation of 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 into full-spectrum CNO capabilities. The key challenge for militaries in East Asia will center on ensuring the security, reliability, and integrity of country’s mission-critical command, control, communications, computers, intelligence, surveillance, and reconnaissance (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.  

Inherently, these challenges will apply to nearly all operational functions and processes that depend in some extent on cyberspace, including *combat support and logistics systems*. A sophisticated cyberattack on these systems would likely result in cascading effects with ramifications on the individual services and their abilities to carry out operational missions. Depending on the magnitude of cyber-attacks 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. The ability to respond and recover from a major cyber-attack will be determined by 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.  

In the long-term, the deepening socio-economic interdependencies and information architectures integrated in nearly all aspects of civilian governance (i.e. energy systems, communications, water, transportation, finance, etc.) could be to varying levels compromised through various cyber-enabled operations. Consequently, the continuously evolving character and reliance on cyberspace in both 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 U.S. 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 military innovation - 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, U.S. strategic partners and allies in East Asia will have to 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 East Asia.

---