中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

VOLUME 16 • ISSUE 11 • JULY 6, 2016

IN THIS ISSUE:

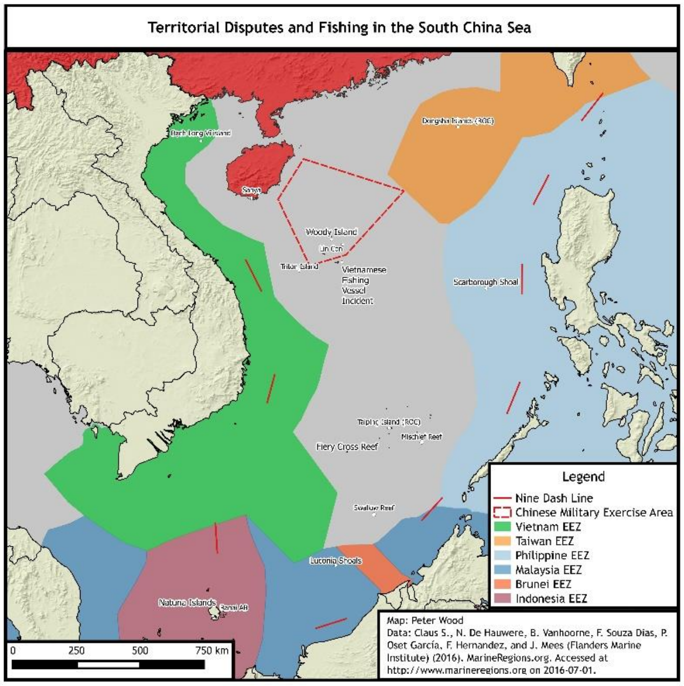
In a Fortnight:
China’s Great Fishnet

With the announcement that the Permanent Court of Arbitration will rule on July 12 on its case between the Philippine and Chinese governments regarding China’s territorial claims in the South China Seas, tensions in the area are coming to a head (Court of Arbitration, June 29). On July 3, China’s Maritime Safety Agency released a notice to mariners declaring a sizeable part of the South China Sea off-limits between July 5–11 for military exercises (China Maritime Safety Administration, July 3; see map). The off-limits area is more than 86,000 square kilometers, larger than South Carolina. China has also increased its tempo of public statements and rebuttals regarding the court case in recent months (*China Brief*, June 21). The various involved parties have marshalled lawyers, spokespeople and military vessels. China has also bankrolled and organized a massive militia of fishermen to support their claims. **[1]**

Though laws, Freedom of Navigation Operations and ancient maps have been the primary means of contest in this debate, insufficient attention is being given to arguably the most important issue: fish. As a major consumer of fish stocks, China is deeply interested in securing the fishing rights for itself and controlling access of other nations to the area. Ensuring adequate future supplies of fish—both domestically through aquaculture and externally through enforcement of territorial claims over large swathes of open sea—contributes to Chinese food security, which has repeatedly been listed a major priority for China’s top leaders (*China Brief*, March 8; *China Brief*, June 1). Less of a wall, Chinese claims—including the Nine Dash Line—are more of a Great Fishnet swallowing the South China Sea.

Fish is a major source of protein for all Southeast Asian nations. It supplements diets dominated by rice to add important amino acids and other nutrients necessary for growth. Many of these nations, particularly Vietnam and the Philippines, have high population densities and comparatively low amounts of arable land, further magnifying the importance of food sources outside traditional crops. Unsurprisingly, these two countries have been among the most vocal in pressing their competing maritime claims with China.

China itself has a large coastline, and a tremendous number of Chinese citizens rely on or are in involved in supporting the world's largest fishing fleet. Many ships operate globally to access less contested fishing grounds, but a host of smaller vessels and subsistence fishermen plough the seas closer to home. **[2]** China's coastal population is enormous: Guangdong province, which forms the northern rim of the South China Sea, is itself home to over 104 million people (Guangdong Government Statistics, May 11, 2011). With the semi-official remit of the Nine-Dash-Line and the might of the Chinese Coast Guard and navy behind them, Chinese fishermen have frequented the exclusive economic zones of many of China's neighbors.


Territorial Disputes and Fishing in the South China Sea

Map: Peter Wood
Data: Claus S., N. De Hauwere, B. Vanhoorne, F. Souza Dias, P. Oset García, F. Hernandez, and J. Mees (Flanders Marine Institute) (2016). MarineRegions.org. Accessed at http://www.marineregions.org on 2016-07-01.

As seen from the map, the "Nine-Dash Line"—even only the area around land features within its borders is included, would dramatically shrink the Exclusive Economic Zones (EEZs) of the countries rimming the South China Sea, and with it, their fishing zones. Just as China's demand for reliable sources of grain is driving a push for diversification and reform of agriculture in China, the demand for fish is going to be a powerful force driving Chinese policy toward the South China Sea. China's neighbors are not just responding to a destabilizing reinterpretation of international law—they are facing a much more powerful neighbor maneuvering to monopolize key fish stocks, an indispensable source of protein for their citizens.

In late March, confrontations between Indonesian Coast Guard vessels and Chinese fishermen escalated to the point that the Indonesian government formally summoned the Chinese ambassador (*China Brief*, March 25). Tensions subsided but recently spiked again, as Indonesian Coast Guard vessels seized and subsequently destroyed Chinese fishing vessels caught operating in Indonesian Waters (Sina, June 25). Similarly, Malaysia has reported that over 100 Chinese vessels were operating in its coastal waters off near Luconia Shoals in the southeastern portion of the South China Sea (Straits Times, March 26). In late May, Vietnamese state media recounted an incident south of Woody Island (永兴岛) during which a Vietnamese fishing vessel was struck repeatedly by what appears to have been a Chinese Coast Guard Vessel (Truoi Tre News, June 19; see map).

Much of the attention on the South China Sea has been directed toward its implications for maritime security, freedom of navigation, and "militarization" of the area. But for many of the disputants, the eventual resolution of the disputed claims, and its implications for fishing rights, represents an existential threat: food security. Observers of the conflict and policy makers involved in proposing solutions should keep this issue at the forefront of their minds. China's firm stance on the "Nine-Dash Line" and the South China Sea more generally has its roots in core issues like the legitimacy of the Communist Party, historical issues involving its territory and foreign relations. However, the importance of the South China Sea's bounty of marine protein as a *casus belli* should not be discounted.

Notes

1. Andrew Erickson and Connor Kennedy, "*China's Maritime Militia*," CNA, July 29, 2015. https://www.cna.org/cna_files/pdf/Chinas-Maritime-Militia.pdf
2. Zhang Hongzhou, *"China's Fishing Industry: Current Status, Government Policies, and Future Prospects,"* CNA, July 29, 2015. https://www.cna.org/cna_files/pdf/China-Fishing-Industry.pdf

China's Blueprint for Sea Power

By Andrew S. Erickson

Powered by the world's second largest economy and defense budget, China has implemented a consistent, incremental strategy of upholding its outstanding territorial and maritime claims in the Near Seas (Yellow, East, and South China Seas), while more gradually developing an outer layer of less-intensive capabilities to further its interests and influence farther afield. In March, China further enshrined its turn toward maritime power in the 13th Five-Year Plan.

Although China is often frustratingly opaque to outside analysts with respect to specific military hardware capabilities, the military strategy that informs the People's Liberation Army's (PLA) organization and use of its forces is often far more transparent in its broader objectives and dimensions. Demonstrably authoritative PLA texts that discuss these topics, such as the Academy of Military Science's (AMS) multiple versions of *Science of Military Strategy* (战略学, or SMS), are increasingly joined by official Defense White Papers (DWP) as well as a wide range of other publications and data. **[1]** Considering this material together offers a fairly clear picture of where China stands militarily and its intended course for the future.

Maritime security development is at the geographic and operational forefront of Chinese military development. The aforementioned sources accurately portray the PLA Navy (PLAN) as undergoing a strategic sea change in recent years. Similarly transforming to support comprehensive efforts at sea are China's maritime law enforcement (MLE) forces and its maritime militia. The PLAN, soon to be the world's second largest blue water navy, retains a lead role in the Near Seas. The world's largest blue water coast guard and largest maritime militia share important responsibilities—typically in coordination with the PLAN. Beijing is pursuing a clear hierarchy of priorities whose importance and realization diminishes sharply with their distance from mainland Chinese territorial and maritime claims, while engaging in a comprehensive modernization and outward geographic radiation of its forces. This is part of a layered pattern dating to the earliest days of the Party and its Army, even before it established the People's Republic in 1949. Having consolidated all its more-pressing inner geographic rings of interests in ensuing decades, Beijing can finally focus on furthering its unresolved claims in the Near Seas, and promoting its broader interests beyond them.

China's Hierarchy of Security Priorities

1. Party Leadership
2. Party-State Administration
3. Governance of Core Han Homeland
4. Stability in Ethno-Religious Minority Borderlands
5. Integrity of Land Borders
6. Upholding and Furthering Near Seas Claims
7. Addressing Far Seas Interests

This ongoing sea change is encapsulated particularly clearly in the 2013 and previous editions of SMS, as well as China's 2015 DWP. This first-ever defense white paper on strategy offers the latest high-level doctrinal and strategic expression of Beijing's military development efforts—and indicates more specifically how SMS (2013) is being refined, amplified, and implemented in practice. In particular, it suggests that China's leadership is embracing new realities and displaying new sophistication in prioritizing and envisioning maritime force development, integration, and utilization across a wide range of peacetime and wartime contingencies. It charges the PLA with safeguarding China's increasingly complex, far-ranging interests through an ideally seamless comprehensive approach combining peacetime presence and pressure with combat readiness. There is unprecedented emphasis on maritime interests and operations to uphold them—imposing new challenges and opportunities on China's maritime forces, with the PLAN at their core. The DWP goes so far as to state that the "traditional mentality that land outweighs sea must be abandoned… great importance has to be attached to managing the seas and oceans and protecting maritime rights and interests." It underscores determination to strengthen Chinese "strategic management of the sea" and "build a combined, multi-functional and efficient marine combat force structure."

These official publications build logically on predecessor documents and are echoed rather consistently in other contemporary documents. Reflective of China's increasing naval and maritime developments at home and growing interests and activities abroad, they embody no less than an ongoing Chinese transformation from a land power into a hybrid land-sea power. This reality is underscored by the unprecedentedly robust maritime content in the 13th Five Year Plan (FYP) (2016–20) passed by the National People's Congress and released on March 17, 2016. Operationalizing many of the concepts discussed in the aforementioned publications, this most authoritative and comprehensive of all national planning documents declares that China will:

1. Build itself into a "maritime power"
2. Strengthen the exploration and development of marine resources
3. Deepen historical and legal research on maritime issues
4. Create a highly effective system for protecting overseas interests and safeguard the legitimate overseas rights/interests of Chinese citizens and legal persons
5. Actively promote the construction of strategic strong points (战略支点) for the "21st Century Maritime Silk Road"
6. Strengthen construction of reserve forces, especially maritime mobilization forces **[2]**

Given the strong demonstrable link between China's official writings about military and naval strategy and its ongoing implementation of much of their content in practice, these vital texts offer signs of Beijing's past, present, and future course and speed at sea.

Chinese Naval Strategy under Xi

Chinese doctrinal publications and the "facts on the water" that they inform are noteworthy for both their strategic consistency and their rapidity of physical implementation (in terms of hardware and personnel development and deployment, as operational employment). Whereas SMS 2001 was a sweeping intellectual treatise outlining both the general rationale for things that China was beginning in practice and many less tangible aspirations for further progress, the 2013 edition describes in more acute, compelling detail a significant step forward in maritime security development that is clearly unfolding in practice before the watchful eyes of foreign observers. The latest iteration of *Science of Military Strategy* thus builds on its predecessors as part of a logical continuum. Several differences between the 2001 and 2013 editions merit emphasis:

- Shift from "Local War under High Tech Conditions" to "Local War under Informatized Conditions"
- Adoption of a two-layered strategy: "Near-Seas Defense, Far-Seas Operations" (近海防御、远海防卫)
- Enhancing "active defense" to distance potential enemy operations from China's shores
- Expanding strategic space in keeping with national interests
- Unprecedented stressing of the need to engage in "strategic prepositioning"
- Increased emphasis on MOOTW and international maritime contributions

SMS 2013 argues that China must build geographically outward on its existing doctrine of "active defense" by "carrying out forward edge defense" and therefore extend the potential culminating point of any future conflict as far from the mainland as possible. In an era in which China's national interests have "surpassed the traditional territorial, territorial sea, and territorial airspace scope to continuously expand toward the periphery and the world, continuously extending toward the ocean, space, and electromagnetic space," and in which "the main war threat has switched from the traditional inland direction toward the ocean direction," the PLA "must expand its military strategic view and provide strong and powerful strategic support within a greater spatial scope to maintain [China's] national interests." Under these conditions, Chinese strategists fear specifically that a "strong adversary" (a euphemistic reference to the United States, perhaps working with one or more allies) will project "its comprehensive distant combat superiority in the oceanic direction" to threaten China's interests. Accordingly, "the difficulty of guarding the home territory from the home territory and guarding the near seas from the near seas will become greater and greater." Therefore, the PLA must "externally push the strategic forward edge from the home territory to the periphery, from land to sea, from air to space, and from tangible spaces to intangible spaces."

The concept of "forward edge defense" articulated in SMS 2013 has clear naval-maritime implications; it feeds the general call for strategic capabilities projection radiating coast-, sea-, and ocean-ward from China's continental core, and specifically for the establishment of a Chinese "arc-shaped strategic zone that covers the Western Pacific Ocean and Northern Indian Ocean." Should China lose the strategic initiative, this "protruding" arc can become a "strategic outer line" whose deterrence, absorption, and control is enabled by "operations with the mainland and the coastal waters as the strategic inner line." This relates to a formulation appearing increasingly in this and other Chinese sources: "using the land to control the sea, and using the seas to control the oceans" (以陆制海, 以海制洋). In keeping with the outward expansion of Chinese defense parameters, the first half of this phrase (representing a continental approach to maritime security) has long been employed in Chinese writings, but the second half (befitting Beijing's emerging hybrid land-sea power posture) is newer in its emphasis.

PLA strategists see the PLA Navy as now being in its third historical period, in which the previous period's strategy of "near-seas defense" has been joined by an additional outer layer of "far-seas protection" (远海护卫). As the 2015 DWP elaborates, "The PLAN will continue to organize and perform regular combat readiness patrols and maintain a military presence in relevant sea areas" while also developing growing power projection capabilities as a limited blue water navy.

This is clear doctrinal enshrinement of the hierarchically prioritized, layered approach to Chinese maritime/military development and deployment that may be observed inductively from a plethora of data points and sources. It is precisely this current concept that the PLAN and its sister sea services are presently in the process of growing into and fulfilling.

Beginning in 2004 with Hu Jintao's assigning "New Historic Missions" to the PLA and a corresponding new strategy to the PLAN, the third era in the service's development "gradually extends the strategic front lines from the near-seas outward into the far-seas, where national survival and development interests [are also at stake]." Answering this call is requiring the PLAN to "deal with multivariate maritime threats" and "accomplish diverse maritime missions."

As part of "preparation for military struggle" in order to safeguard China's "expanding national interests," the PLAN must "deal with informatized maritime local war." The 2015 DWP further emphasizes "winning informatized local wars" (打赢信息化局部战争) as the new "basic point" of China's latest "military strategic guideline." In an indication of growing emphasis on furthering outstanding island and maritime claims in the Near Seas, the document stresses that "basic point for [Preparation for Military Struggle] will be placed on winning informatized local wars, highlighting maritime military struggle and maritime PMS." Under these conditions, *Science of Military Strategy* (2013) assigns the PLAN eight "strategic missions":

1. Participate in large-scale operations in the main strategic axis of operations.
2. Contain and resist sea-borne invasions.
3. Protect island sovereignty and maritime rights and interests.
4. Protect maritime transportation security.
5. Engage in protecting overseas interests and the rights/interests of Chinese nationals.
6. Engage in carrying out nuclear deterrence and counterattack.
7. Coordinate with the military struggle on land.
8. Protect the security of international sea space.

In order to fulfill its eight "strategic missions," the PLAN must make five specific efforts:

1. Comprehensively strengthen the construction of maritime information systems.
2. Accelerate the navy's development of next-generation main battle armaments.
3. Strive to develop sea-based strategic nuclear forces.

4. Adjust maritime force deployment and battlefield layout.
5. Concentrate on the features of future naval war to optimize force structure.

Finally, with respect to preparing for its potential strategic use in war in accordance with China's overall maritime combat capabilities under informatized conditions, AMS strategists argue that the PLAN should "highlight" four aspects in its preparations for future naval operations: operational depth, offensive operations, Integrated Joint Operations, and asymmetric warfare.

These admonitions are grounded conceptually in the continuous, progressive geographic and conceptual expansion of China's national security interests. In an operational sense, strategic space clearly helps create depth for the implementation of China's active defense strategy and the amorphous lines and areas at sea wherein it would wage maritime combat, including maritime people's war. However, a more complex question of interpretation remains concerning how precisely Xi is directing his military/maritime forces and related actors to address China's expanding interests.

In this vein, SMS 2013 calls for "relying on one's home territory while moderately expanding the strategic space" (依托本土适度拓展战略空间), a phrase with numerous possible interpretations. The crux of the matter is the term "本土," which SMS 2013 employs frequently but does not define directly, and the physical locations to which it refers. Given China's emphasis officially on the "indisputable" nature of its sweeping claims in the South China Sea in this document and elsewhere, this ambiguous yet potentially broadly inclusive term may refer not only to mainland China, but also all South China Sea islands, reefs, and other features claimed by Beijing. The "favorable conditions" and "laying a solid foundation" to which the authors allude could thus refer to increasing presence in claimed areas to demonstrate administration and enforcement, all the better to solidify the territorial foundation for forward-supported strategic expansion. China's aforementioned "island building" and maritime fortification activities would follow directly from such an approach.

At a minimum, the authors envision a very significant further outward expansion of China's interests, capabilities, and forces. This involves a Chinese maritime theater concept not widely discussed in previous authoritative Chinese documents: the idea of a dual Indo-Pacific focus for China's navy, as encapsulated in the aforementioned "arc-shaped strategic zone that covers the Western Pacific Ocean and Northern Indian Ocean." This zone is now termed the "Two Oceans region/area" (两洋地区) in authoritative sources, and is described as "mainly" including "the Pacific Ocean, Indian Ocean, as well as the littoral regions of neighboring Asia, Africa, Oceania, North America, South America, and Antarctica, etc., with a total area occupying over 50 percent of the globe; within which the Two Oceans have a total area of 254.6 million square meters, occupying 71 percent of the global ocean area."

The authors of SMS 2013 describe the Two Oceans region as being extremely important to China and its security interests. It represents "a crucial area in influencing" China's "strategic development and security in the future" as well as "the intermediate zone of our entrance into the Atlantic Ocean region, Mediterranean Sea region, and Arctic Ocean region." In accordance with the globalizing nature of China's activities, they declare, its "national interests will surpass in an extremely large manner the traditional territorial land, territorial sea, and territorial air scope, while the Two Oceans region will become the most important platform and medium." On this basis, Chinese actors "will create conditions to establish ourselves in the Two Oceans region, participate in resource extraction and space utilization of the oceans, and boost development in the two polar regions."

To be sure, the authors allow, new challenges and "security threats" of both a traditional and a non-traditional nature should be expected to accompany this sweeping geostrategic expansion, "especially [from] the oceanic direction." These interrelated factors, in turn, offer an impetus for further security development, in a manner that is likely to offer continued rationale for concerted qualitative and quantitative development of the PLAN for years to come. Even amid continued hierarchical prioritization, Chinese strategists appear to have left the PLAN considerable geographic "room to grow" for even its most important operations: literally half the globe!

Conclusion: Sea Change Underway

Analyzed in juxtaposition over time, and compared against specific empirical manifestations of Beijing's burgeoning efforts in the maritime domain, China's major doctrinal publications and public statements reveal a sea change in strategic priorities and emerging capabilities to further them. China retains an incremental approach, in keeping with a disciplined hierarchy of national security priorities, but this layered development is already making major outward-radiating waves as the Middle Kingdom turns increasingly seaward as a hybrid land-sea great power.

Whether viewed deductively from strategic intentions, or inductively from development, operational, and tactical actions, China's increasingly-modernized and -integrated maritime forces—centered on the PLAN—are pursuing a two-fold effort: intensive "near seas active defense" of outstanding island and maritime claims on China's maritime periphery, coupled with "far seas protection" of more diffuse, diverse interests beyond.

Real-world developments, particularly ongoing Chinese activities vis-à-vis the South China Sea, suggest that the strategic thinking embodied in the various iterations of SMS, the DWP, and related official publications and statements is strongly indicative of actual PLA planning and action—both now and in the future. Analysts of China's armed forces in general, and its navy in particular, should therefore continue to consider in-depth what some of Beijing's latest conceptual thinking may mean increasingly in practice in coming years. In that regard, three concepts in particular should enjoy top priority for further explication: Chinese "home territory" and its role in force projection, the nature and expansion of Chinese "strategic space," and activities and prioritization within the "Two Oceans" strategic zone envisioned for heightened naval operations.

Dr. Andrew S. Erickson is Professor of Strategy in, and a core founding member of, the U.S. Naval War College's China Maritime Studies Institute. He serves on the Naval War College Review*'s Editorial Board. Since 2008 he has been an Associate in Research at Harvard University's John King Fairbank Center for Chinese Studies. Erickson received his Ph.D. and M.A. from Princeton University and studied Mandarin at Beijing Normal University's College of Chinese Language and Culture. He can be reached through* www.andrewerickson.com.

Notes

1. Academy of Military Science Military Strategic Research Department [军事科学院军事战略研究部], *The Science of Military Strategy* [战略学] (Beijing: Military Science Press, 2013); "China's Military Strategy" [中国的军事战略] (Beijing: State Council Information Office, PRC, May 2015), http://www.81.cn/dblj/2015-05/26/content_6507373.htm.
2. Su Xiangdong [苏向东], Editor, China's Five Year Plan for Social and Economic Development (Full Text) [中国国民经济和社会发展第十三个五年规划纲要 (全文)], Xinhua, March 17, 2016, http://www.china.com.cn/lianghui/news/2016-03/17/content_38053101.htm, http://www.china.com.cn/lianghui/news/2016-03/17/content_38053101_11.htm, http://www.china.com.cn/lianghui/news/2016-03/17/content_38053101_14.htm, http://www.china.com.cn/lianghui/news/2016-03/17/content_38053101_20.htm. The author appreciates Ryan Martinson's bringing these documents to his attention.

***

Growing PLA Transparency as a Means of Employing Soft Power, Part 1: PLA Internal Signaling Since the 18th Party Congress

By Kenneth Allen

As China emerges during the 21st Century as a strong regional power with a growing global footprint, the role of the People's Liberation Army (PLA) as a means of employing "military soft power" (军事软实力) has garnered close scrutiny both internally and externally from multiple perspectives, including the development and deployment of advanced weapons and equipment, as well as being involved in an increasing number and scope of domestic and international training exercises and drills. This article, the first of a two-part series, examines the PLA's use of soft power for both internal and external signaling.

It appears that China did not formally apply the concept of "military soft power" to the People's Liberation Army (PLA) until Hu Jintao took over the leadership in September 2004. **[1]** Under Hu and Xi Jinping, who took over power in 2012, one of the key aspects of soft power has been the increasing level of military transparency (透明) concerning not only interaction with foreign militaries but also internal PLA issues.

Disagreements on the issue of transparency have always been at the core of China's foreign military relations. For example, the U.S. Department of Defense's *Annual Report to Congress on the Military and Security Developments Involving the People's Republic of China 2014* stated:

> Although the dialogue between the United States and China is improving, outstanding questions remain about the rate of growth in China's military expenditures due to the lack of transparency regarding China's intentions.
>
> It is difficult to estimate actual PLA military expenses due to China's poor accounting transparency and incomplete transition from a command economy. China's published military budget omits several major categories of expenditure, such as procurement of foreign weapons and equipment.
>
> China's lack of transparency surrounding its growing military capabilities and strategic decision-making has led to increased concerns in the region about China's intentions. Absent greater transparency from China and a change in its behavior, these concerns will likely intensify as the PLA's military modernization program progresses. **[2]**

In September 2014, U.S. Assistant Secretary of State Daniel Russell, the senior U.S. diplomat for East Asia, stated, "Frankly, the lack of transparency in China's military modernization is the source of some concern to its neighbors. And we believe that all of the region, including China, would benefit from increased transparency" (*Reuters*, September 13, 2014).

Although the PLA's last two biennial Defense White Papers did not specifically address the issue of transparency, a commentary in *China Military Online* on the publication of the 2012 Defense White Paper by Rear Admiral Guan Youfei, director of MND's Foreign Affairs Office stated:

> "It should be said that the transparency of the PLA is consistent with the reality of our national and military situation. Military transparency is important for national security. The extent, method, content and timing of transparency to the outside world should be determined according to each country's safety situation and no country is absolutely transparent when it comes to military affairs. In recent years, the Chinese military has adopted a series of measures to open itself to the world, such as establishing a news spokesperson system for MND, opening a website of MND (http://eng.mod.gov.cn), and inviting foreign correspondents to visit

> and interview, all of which were unimaginable ten years ago. It could be said that China is very transparent on military affairs" (China Military Online, April 17, 2013).

Opening of the PLA to the Public

In order to address foreign concerns about transparency, the PLA has implemented several administrative and organizational solutions since the mid-2000s. Specifically, the PLA has gradually expanded the content of its eleven biennial Defense White Papers that was first published in 1998, established the Ministry of National Defense (MND) Information Office in September 2007, and created a new MND website, with both English and Chinese versions, that came online on August 20, 2009 (*China Daily*, July 23, 2009). In 2007, MND began holding ad hoc press conferences, which became monthly in 2012. **[5]** In August 2009, MND created official websites in Chinese (www.mod.gov/cn) and English (http://eng.mod.gov.cn/), which is also known as "*China Military Online*" or chinamil.com. In addition, the PLA created separate Chinese websites for the General Logistics Department (GLD), General Armament Department (GAD), Navy (PLAN), Air Force (PLAAF), Second Artillery Force (PLASAF), and all seven military regions (MR), each of which used 81.cn (e.g., August 1st or *bayi*) as the base. **[6]** In addition, the PLAN, PLAAF, PLASAF, and MR newspapers, each of which were previously for internal use (内部) or military use (军内) only, removed those restrictions and became available publicly through a post office subscription. However, major changes occurred to several of the newspapers in January 2016 as a result of the PLA reorganization. Specifically, the individual MR newspapers ceased publication that month, and, similarly, the GLD, GAD, and MR websites also disappeared and have been replaced by a new general website (军报记者 / http://jz.81.cn) and separate websites for the new Logistics Support Department, Equipment Development Department, Army Headquarters, and each of the theater commands (hq.81.cn/; zf.81.cn/; http://army.81.cn/; db.81.cn; nb.81.cn; xb.81.cn; bb.81.cn, and zb.81.cn;). In addition, a second military website for video (中国军视网 / http://tv.81.cn/) was also created on December 29, 2015. In addition, China Central Television (CCTV) has greatly increased its coverage of PLA activities.

In 2009, the PLA component of Xinhua began publishing a new 110-page quarterly journal in Chinese and English entitled *China Armed Forces* (中国军队). Since January 2012, it has been published bimonthly. Certain volumes have focused on specific topics, such as the military service system and various anniversaries, including the founding of the PLA (1927), PLAN (1949), PLAAF (1949), and the end of World War II (1945). Starting in 2013, the first issue for each year has had lengthy articles that review key PLA activities for the previous year, including military relations, joint and combined exercises, peacekeeping operations, and military operations other than war (MOOTW) activities, as well as some important policy and weapons issues. The same information is also available on various Chinese websites.

Key PLA Issues for 2013 through 2015

Although the PLA has clearly expanded the release of its overall information over the past several years, the remainder of this article focuses on information that the PLA published at the end of 2013 through 2015 that it identified as its top issues during the previous year.

The primary sources for this information is *China Armed Forces* magazine and various military news outlets. Specifically, the first issue of *China Armed Forces* magazine in 2014 carried two lead articles entitled "Highlights of China's Military Diplomacy in 2013" that identified the top nine military relations events and "Military News in 2013" that is a mix of policy, weapons, and military relations. **[7]** This was the first time since the magazine was created in 2009 that it listed these accomplishments, which indicates that military diplomacy has become a more important and transparent element of the PLA.

On December 26 and 29, 2014, MND's official website published "Ten Breakthroughs of China's Military Diplomacy in 2014," which were also published in the first volume of *China Armed Forces* in 2015. **[8]** According to the article, "In 2014, the Chinese military played a more active role in assuming the responsibilities of a major country, deepened its relations with the militaries of many countries, aired its voices more loudly, and carried out military drills in a more practical way. If we have to summarize China's military diplomacy in 2014 with one sentence, the best choice may be 'military shows more major-country style'."

On December 30, 2015, the newly created China Military Network published an article that identified the top ten military activities during 2015 (China Military Online, December 30, 2015). A list of 39 key activities were identified which can be organized into the following seven categories, some of which clearly overlap:

1. Combined Training, Meetings, and Agreements with Foreign Militaries
2. Joint and Combined-arms PLA Exercises and Training
3. PLA Navy Activities
4. PLA Air Force Activities in the East China Sea ADIZ
5. UN Peacekeeping
6. Army Building and Discipline
7. Defense Industry and Equipment.

The following sections address the latter two categories, which are focused on domestic military affairs.

Army Building and Discipline

One of the most prolific themes has dealt with what the PLA calls "army building" (军队建设), which includes everything from acquiring weapons and equipment to developing doctrine and dealing with personnel and organizational issues, especially problems with corruption. Because this is an area that the central leadership is eager to spread information about—and enforce its directives—there is a higher degree of transparency and greater media attention given to it. The following bullets lay out the top ten issues involving army building the PLA identified for 2013 through 2015.

1. Xi Jinping sets new goals for army building during the First Plenum of the 12th National People's Congress (NPC) in March 2013, where he urged the armed forces to be "absolutely loyal" to the Party, to sharpen their fighting capabilities, and abide by discipline in order to elevate the country's defense and army building. **[9]**
2. During the Third Plenum of the 18th Party Congress in November 2013, "The Decision on Major Issues Concerning Comprehensively Deepening Reforms by the Party Central Committee," which focused on developing theories and strategic guidance, reforming the organizational structure, and deepening military-civil fusion.
3. In April 2013, the eighth biennial Defense White Paper provided true unit designators for all 18 group armies for the first time.
4. In 2013, the PLA adopted a series of measures to strengthen management, that focused on managing expenses related to corruption, including confiscating 23,231 illegal homes and reducing the number of official cars by 25,510.
5. During 2014, Xi led a campaign to root out corruption in the PLA, which included a meeting of the Chinese Communist Party (CCP) Politburo in June.
6. In October 2014, Xi led a meeting in Gutian, Fujian Province, to commemorate the 85th anniversary of the first Gutian Meeting. The meeting focused on the Party's absolute leadership over the PLA and the goal of eliminating corruption in the PLA.
7. From November 24–26 2015, Xi chaired a CMC meeting concerning the PLA's reorganization (军队改革), which was then implemented.
8. During 2015, the military and PAP implemented the "Three Stricts and Three Honests" (三严三实), which is an internal education campaign led by the CCP aimed at improving the ethical conduct of Party officials and "improving political ecology" (China.org, June 15, 2015).
9. On September 3, 2015, Xi announced that the military would implement a 300,000-

man force reduction, which is the eleventh force reduction and reorganization since 1952.

10. On May 26, 2015, China issued its ninth biennial Defense White Paper, which focused on military strategy.

Defense Industry and Equipment

Although the acquisition of PLA weapons and equipment is one of the black holes in China's military transparency, the PLA identified three key issues during 2013 to 2015, most of which, ironically, was based on foreign reporting. By using foreign media reports, Chinese state media is able to discuss what would otherwise be sensitive information, and frame the development of Chinese military capabilities in a way that is palatable to the state.

1. During 2013, China's defense industry in conjunction with the PLA displayed and deployed several new types of equipment and weapon systems, including showing the Y-20 and deploying new types of destroyers, as well as command and escort vehicles.
2. During 2014, the PLAN was scheduled to commission several vessels from China's shipbuilding industry, including a Type 052D destroyer and Type 056 corvette. Supposedly, dozens of Type 056 corvettes are under construction in five shipyards.
3. During 2014, China and Russia signed several military trade deals, including contracts involving fighters and air defense missiles, as well as bilateral cooperation on large aircraft, highly sensitive and advanced navigation satellites, and nuclear energy.

Conclusion

Most foreign news articles tend to focus on the PLA's growing arsenal of weapons and China's "aggressive behavior" in the East China Sea and South China Sea, as well as its growing diplomatic, economic, and military relations around the world. **[11]** The information identified by the PLA in this article has clearly helped shape the view of the PLA from a military soft power perspective, and forms an important part of its domestic propaganda mechanism, by being transparent on issues about which it wants to increase social attention to, such as "military building" and framing information about its developing military capabilities through the use of foreign media attention.

Part two will examine the impact of Joint and combined-arms PLA exercises and training on transparency and soft power.

Kenneth W. Allen is a Senior China Analyst at Defense Group Inc. (DGI). He is a retired U.S. Air Force officer, whose extensive service abroad includes a tour in China as the Assistant Air Attaché. He has written numerous articles on Chinese military affairs. A Chinese linguist, he holds an M.A. in international relations from Boston University.

Notes

1. Kenneth Allen, *Trends in People's Liberation Army International Initiatives under Hu Jintao*, in Roy Kamphausen, David Lai, and Travis Tanner, eds., *Assessing the People's Liberation Army in the Hu Jintao Era*, United States Army War College Press, April 2014.
2. *Annual Report to Congress on the Military and Security Developments Involving the People's Republic of China 2014*, U.S. Department of Defense, April 24, 2014, found at http://www.defense.gov/pubs/2014_DoD_China_Report.pdf.
3. Xiao Jingmin, "A Theoretical Exploration into the Soft Power in China's National Defense," and "The Ministry of National Defense (MND) will launch an official bilingual website on August 1," http://china-defense.blogspot.com/2009/07/ministry-of-national-defense-mnd-will.html. The literal translation for the Information Office is the News Service Bureau and it is just one of several MND bureaus.
4. Information on the monthly conferences, which are usually held on the last Thursday

of the month, is based on a review of the MND website's press briefings tab, found at http://eng.mod.gov.cn/Press/index_3.htm.

5. The websites, some of which no longer exist, are as follows: GLD (zh.81.cn), GAD (zz.81.cn), PLAN (navy.81.cn), PLAAF (kj.81.cn), PLASAF (ep.81.cn), Shenyang MR (sy.81.cn), Beijing MR (bj.81.cn), Lanzhou MR (lz.81.cn), Jinan MR (jn.81.cn), Nanjing MR (nj.81.cn), Guangzhou MR (gz.81.cn), and Chengdu MR (cd.81.cn).
6. Luo Zheng, "Highlights of China's Military Diplomacy in 2013" (2013 中国军队走处国门亮点频现), *China Armed Forces*, No 25, Vol.1, 2014, pp. 16–19. Editorial Department, "Military News in 2013" (2013 年中国十大军事新闻), No 25, Vol. 1, 2014, pp. 13–15.
7. Yao Jianing, ed., "Ten breakthroughs of China's military diplomacy in 2014" parts 1 and 2, *China Military Online*, December 26 and 29, 2014, respectively, found at http://english.chinamil.com.cn/news-channels/2014-12/26/content_6286046.htm and http://english.chinamil.com.cn/news-channels/2014-12/29/content_6288402.htm. The Chinese article, which included all ten events was found at http://www.81.cn/jmywyl/2014-12/25/content_6284840.htm. The article noted that the ten breakthroughs are listed in chronological order not by precedence. Kong Xianglong, "Top 10 Topics Regarding China's Army in 2014" (中国军队 2014 年十大热点话题), *China Armed Forces*, No. 31, Vol. 1, 2015, pp. 6–11.
8. Zeng Xingjian and Hong Yihu, "Passing the Strait of Magellan," *China Armed Forces*, No. 24, Vol. 6, 2013, pp. 80–83. Official Chinese English-language publications, such as the biennial *Defense White Paper*, refer to the South Sea Fleet as the Nanhai Fleet.
9. Note: China's "armed forces" (武装力量) is composed of three components: 1) the PLA, 2) the People's Armed Police (PAP), and 3) reserves and militia. It is often just referred to as the "military" (军队).

Africa: China's Laboratory for Third World Security Cooperation

David H. Shinn

China's interests and exposure in Africa have grown exponentially over the past two decades. China became Africa's largest trading partner in 2009 and continues to hold the lead by a wide margin. China is the largest bilateral funding source for infrastructure projects, nearly all of which are tied to construction by Chinese state-owned companies using a percentage of Chinese labor. Foreign direct investment in Africa according to China's official statistics totaled $32.35 billion at the end of 2014, although some observers put the number much higher. **[1]** In recent years, China's official aid to Africa has been averaging about $2.5 billion annually (China's Foreign Aid, 2014). While there is no precise number for Chinese nationals living in and visiting Africa at any given time, senior Chinese officials usually put the figure at more than one million and some analysts say there may be as many as two million. At the end of 2014, there were about 200,000 Chinese working in Africa on contracts and another 62,000 providing services under aid programs. **[2]** Most of the other Chinese in Africa are businesspersons, independent entrepreneurs, small traders and tourists.

Attacks on Chinese nationals in Africa are not new; it is a challenge China has faced for more than a decade (*China Brief*, April 2, 2009). China's growing physical presence has resulted, however, with more Chinese in harm's way and, on occasion, as specific targets. The continuing attacks have drawn increasing criticism from the Chinese public and caused the government to consider additional measures to counter the problem. China's physical presence and investments in Africa face the same challenges as other countries. The wake-up call came in 2011 when China evacuated almost 36,000 nationals, mostly contract workers, from Libya following the toppling of Muammar Gadaffi's government (SIPRI Policy Paper, June 2014). More recently, three Chinese railway executives died during the terrorist attack in 2015 on the Radisson Blu Hotel in Bamako, Mali that killed 20 persons (Caixin, January 27). In 2016, one Chinese peacekeeper was killed and four injured during a mortar attack on a UN base in northern Mali (MFA, June 1). Al-Qaeda in the Islamic Maghreb claimed responsibility for the attack (Global Times, June 2).

China's Evolving Policy on Protection

For many years, China operated on the basis that it was the responsibility of individual African governments to protect Chinese nationals who encountered security problems in an African country. While China continues to follow this principle, it has learned African governments are not always capable of providing protection. Consequently, China has looked at measures it can take to improve security for its interests and nationals in Africa. An official at a government-affiliated think tank recently commented that China has unique and long-standing political interests in Africa. Its contributions to UN peacekeeping operations and combatting piracy in the Gulf of Aden constitute a veritable laboratory for security cooperation with the Third World. If China's new approach to security in Africa is successful, it can be followed in places like Latin America. **[3]**

China's policy on Responsibility to Protect (R2P), which goes beyond the protection of Chinese nationals overseas, is also evolving. Courtney J. Fung, professor of international relations at the University of Hong Kong, concluded that between 2000 and 2005, China took a hard line against intervention and in defense of state sovereignty. Between 2005 and 2008 it offered limited endorsement of R2P in the Democratic Republic of the Congo, Burundi and Darfur in Sudan. Since 2009, China has considered R2P an ally of sovereignty but spelled out a strict interpretation of the three-pillar strategy of the 2005 World Summit Outcome Document. China argues that states bear primary protection responsibility (Pillar One). It accepts that the role of the international community is to assist states to meet their protection responsibilities (Pillar Two). As for Pillar Three, the use of force through the UN Security Council is appropriate only if peaceful means fail (USIP PeaceBrief, June 2016; SIPRI Policy Paper, June 2014).

Chinese companies historically had a high level of tolerance for political risk in Africa. It was not unusual to find companies operating in regions such as the Niger Delta in Nigeria and the Ogaden region in Ethiopia, where local dissident groups warned all foreign companies to leave. This led to the kidnapping of Chinese nationals in the Niger Delta. In 2007, nine Chinese workers died in crossfire between Ethiopian government forces and those of the Ogaden National Liberation Front at an oil prospection field in eastern Ethiopia (*China Daily*, April 24, 2007). The Chinese company subsequently ended its exploration activities in the Ogaden.

There has been an ongoing debate within the Chinese Ministry of Commerce on the best way to deal with political risk in Africa. It has considered closer collaboration with local and Western companies, cooperation with European security initiatives and even establishing better relations with tribal leaders. The government has also urged Chinese companies to take greater responsibility for assessing political risk and accepting the consequences (Journal of Cambridge Studies, 2012). China's Vice Minister of Commerce, Qian Keming, commented late last year that in 2010 China began to formulate guidelines for security management of overseas Chinese-funded enterprises and personnel, as well as emergency response mechanisms. He noted that the attack on the Raddison Blu Hotel in Mali gave impetus to this effort (MOFCOM, December 2, 2015).

China is also struggling with the issue of using private security companies in Africa. The government does not support Chinese private security companies (PSCs) going abroad. According to China's Criminal Law, the possession of weapons overseas, even in compliance with the laws of a foreign nation, may result in a maximum sentence of seven years in prison. Nevertheless, the Beijing-based Dingtai Anyuan Security Technology Research Institute (鼎泰安元安全防范技术研究院), a PSC, has been doing business in Nigeria for more than ten years but usually hires Western PSCs (Global Times, December 23, 2015). Another PSC, Shandong Huawei Security Group, established the first ever joint venture with a South African company, HW Raid Private Security, to protect Chinese assets and nationals in South Africa (Farmitracker, December 24, 2014). A

Chinese think tank representative confirmed privately that Chinese PSCs are at an early stage of development, have little experience in using guns and are not yet ready to provide the kind of service required in Africa. **[4]**

China's Evolving Role in UN Peacekeeping in Africa

China has assigned more peacekeepers to UN operations in Africa than any other permanent member of the UN Security Council. It currently contributes more than 2,600 troops, police and experts to seven of the nine missions in Africa. Until 2013, China provided only non-combat personnel, mostly engineers, logisticians and medics. China's assignment of an infantry detachment to the UN Stabilization Mission in Mali (MINUSMA) to protect the MINUSMA headquarters and living areas of the peacekeeping forces marked the first foreign deployment of combat troops to a UN peacekeeping operation (Strategic Review for Southern Africa, 2015).

China has significant interests in South Sudan's oil sector. In 2015, as a result of ongoing civil war, China evacuated more than 400 workers with the China National Petroleum Corporation (Sudan Tribune, May 22, 2015). China had previously agreed to send a 700-strong infantry battalion to the UN Mission in South Sudan. This constituted the first ever combat battalion to serve in a UN peacekeeping mission (*China Brief*, November 2, 2015). Equally important, Geng Yansheng, a spokesperson in the Ministry of National Defense, said the Chinese troops "will provide protection to the local people and other countries' personnel engaged in such peaceful activities as humanitarian assistance and economic development" (China Military Online, September 25, 2014). The UN mandate allows the People's Liberation Army (PLA) battalion to protect local and foreign civilians, including Chinese oil workers (UNSC Resolution 2155, May 27, 2014). This policy also underscores that China's evolving approach to African peacekeeping contains a component of self-interest (Growth Research Programme, May, pp. 50–52).

In 2015, President Xi Jinping announced at the United Nations that China will establish a permanent peacekeeping standby force of 8,000 troops and called on the international community to increase support for African peace and stability (Xinhua, September 29, 2015). So far, the standby force has resulted in a proposal to keep in China one brigade of troops (about 2,500) with engineering and medical capabilities available to the UN at all times. China also committed helicopters to the UN mission in Sudan's Darfur region and $20 million a year for ten years to support a new UN Peace and Development Trust Fund (ECFR policy brief, June).

A New Look at Counter-terrorism in Africa

As terrorist groups have expanded across Africa and Chinese nationals have increasingly been affected by the attacks, China has taken a more collaborative approach to counter-terrorism. The deaths over the past year of Chinese nationals in Mali and an armed Chinese police officer at a hotel in Mogadishu, Somalia have driven home the need to take stronger action (*China Daily*, July 27, 2015). China appreciates that terrorism is no longer just an internal threat for its nationals and interests (*China Brief*, June 2). The global terrorist threat may result in the use of special forces outside China, new counter-terrorism laws, greater pressure on foreign governments to crack down on terrorist groups, direct training and material support to foreign governments to reign in terrorists, and participation with other governments in anti-terrorism exercises (*China Brief*, January 26). At the same time, China is constrained by its long-standing principles of non-interference and security through development (OCP Policy Center, March 16).

China's first counter-terrorism law took effect at the beginning of this year (Xinhua, December 27, 2015). It authorizes "exchanges of intelligence information, enforcement cooperation, and international financial monitoring with foreign nations and relevant international organizations." It also authorizes China to assign PLA personnel and the Chinese People's Armed Police Force to participate in counter-terrorism missions outside the country (Counter-Terrorism Law, December 27, 2015).

China's most recent Africa policy paper states that it will support the efforts of African countries and regional organizations to improve counter-terrorism capabilities and fight terrorism, and help African countries develop their economy and root out the causes of terrorism, with the aim to safeguard regional security and stability and promote long-term sustainable development in Africa. In addition, China will strengthen counter-terrorism exchanges and cooperation with the African Union and priority African countries (Xinhua, December 4, 2015).

During a visit to Nigeria, for example, Premier Li Keqiang promised that China will make available information acquired by its satellites and intelligence service to Nigeria's security agencies and provide training of military personnel for combating the Boko Haram terrorist organization (Xinhua, May 18, 2014). China subsequently sold armed drones to Nigeria, which have been used against Boko Haram (*China Daily*, April 21; *China Brief*, June 26, 2015).

China Expands Its Naval Presence in Africa

The modern Chinese navy made only three port calls anywhere in Africa during the 60 years from 1949 through 2009. **[5]** During the five years between 2010 and 2015, PLA Navy ships made at least 38 calls at African ports, 20 of them at Djibouti. **[6]** This sharp increase in PLA Navy activity is attributed largely to China's participation in the Gulf of Aden anti-piracy operation that began in 2008. It became apparent that China needed ports in the region where it could refuel and resupply. But while the threat of piracy in the Gulf of Aden is essentially over, China continues to expand its naval and military presence.

The most dramatic expression of China's growing naval interest is its decision to establish a permanent military facility at Djibouti, which is scheduled for completion in 2017 by the China State Construction Engineering Corporation. China has a long-standing policy of no foreign military bases and is going to great lengths to describe the facility as something less than a military base. Chinese observers call it, for example, a logistic hub for Chinese ships to obtain replenishment and temporary rest. Zhang Junshe, from the PLA Naval Military Studies Research Institute, said it is "far less than a military base in its scale and function" (Global Times, March 15; *China Brief*, January 26). However, most non-Chinese observers believe this facility sounds more like a military base. When asked why China does not proclaim global conditions have changed and it now needs a military base, a Chinese think tank representative responded that "continuity of Communist Party policy" does not permit a break with the long-standing principle of no foreign military bases. **[7]**

Conclusion

China's security policy in Africa is evolving slowly but inexorably toward greater engagement and a more robust physical presence. This is demonstrated in its global security policy changes, participation in the anti-piracy operation in the Gulf of Aden, gradual increase in numbers of personnel assigned to UN peacekeeping operations and the deployment of combat troops, greater attention to cooperation with African countries on counter-terrorism, and more frequent calls in African ports by the PLA Navy. It is most forcefully demonstrated by the construction of a military facility in Djibouti. While China's military engagement in Africa lags well behind that of the United States and France, it has now joined a small group of nations with major security ties to the continent.

David Shinn is an adjunct professor in the Elliott School of International Affairs at George Washington University and former U.S. ambassador to Ethiopia and Burkina Faso. He is the co-author of China and Africa: A Century of Engagement.

Notes

1. China Statistical Yearbook, 2015, section 11-19. The China Global Investment Tracker operated by the American Enterprise Institute and the Heritage Foundation uses higher FDI figures.
2. China Statistical Yearbook, 2015, section 11-22.
3. Author's conversation on May 6, 2016 at the Shanghai Institutes for International Studies.
4. Author's conversation in Shanghai on May 10, 2016.
5. David H. Shinn and Joshua Eisenman, *China and Africa: A Century of Engagement*. Philadelphia: University of Pennsylvania Press, 2012, p. 189.

6. Andrew S. Erickson and Austin M. Strange, *Six Years at Sea . . . and Counting*. Washington: The Jamestown Foundation, June 2015, pp. 123–134.
7. Author’s conversation in Shanghai on May 6, 2016.

***

A Force for Cyber Anarchy or Cyber Order? —PLA Perspectives on “Cyber Rules”

By Elsa B. Kania

In early June, the Eighth Round of the U.S.-China Strategic and Economic Dialogue (S&ED) “welcomed” apparent progress on cyber security, an issue that has been among the most contentious aspects of this bilateral relationship in recent years (U.S. Department of State, June 7). As the official press release noted, the U.S.-China High-Level Dialogue on Cybercrime and Related Issues occurred last December and recently reconvened in June, and the inaugural Senior Experts Group on International Norms in Cyberspace and Related Issues took place this May and will meet again this fall. Since the previous U.S.-China cyber security working group had been suspended after the indictment of 3PLA hackers in May 2014, this resumption of substantive bilateral engagement on these issues constitutes at least an initial step toward the search for common ground on cyber security that these dialogues seek to advance.

This diplomatic progress on cyber issues, which builds upon other recent advances, raises the question of whether shared interests could enable future cooperation between the U.S. and China or strategic competition will persist in this new, anarchic domain. In 2015, Beijing agreed through the UN’s Group of Government Experts consensus report that certain norms and aspects of existing international law, including the UN Charter, do apply in cyberspace. **[1]** During his September 2015 state visit to the U.S., President Xi apparently agreed to restrain Chinese commercial cyber espionage activities and pledged, along with President Obama, to refrain from cyber attacks against civilian critical infrastructure during peacetime (White House Press Office, September 25, 2015). **[2]**

While such outcomes are encouraging, the prospects for future progress on cyber issues must be evaluated in light of the relevant aspects of Chinese, particularly PLA, strategic thinking on cyber/network warfare. **[3]** Unless diplomatic engagement proves able to impact the PLA’s strategic thinking on and constrain its operational approach to “cyber domain military struggle,” the credibility of Beijing’s rhetorical commitments will remain questionable. Of course, the continuation of efforts to address cyber security in Sino-U.S. relations could be critical to ameliorate mutual misperceptions, establish crisis management mechanisms to lessen the risks of escalation, and perhaps ultimately progress toward the formulation of a consensus on potential ‘rules of the road’ for the cyber domain. However, these efforts should be informed by an understanding of the range of views among the relevant strategists and operators within the PLA, which frequently differ appreciably from China’s articulated diplomatic positions on the topic. This analysis is an initial attempt to outline these perspectives, in an effort to understand the likely constraints upon and potential opportunities for agreement between the U.S. and China regarding a future cyber order.

Following the Cyber Rules?

At this point, a number of PLA theorists and strategists, including affiliates of the PLA’s Academy of Military Science (AMS) and National Defense University (NDU), do appear to recognize the importance of formulating basic “cyber rules” (网络规则), as well as some form of “cyber arms control” (网络军备控制). There is evidently a range of views on the topic, including those who argue for highly competitive approaches to cyber norms and those urging greater cooperation. However, existing Western efforts to institutionalize cyber norms and “cyber laws of war” are often viewed with suspicion, even as attempts to secure U.S. “cyber hegemony” (网络霸权). **[4]** For instance, the Tallinn Manual—a NATO-proposed framework for the application of existing international law, including the laws of war, to cyberspace—has been characterized as an indication of hostile intent. The PLA's perception that the U.S. seeks to reinforce its strategic advantage, rather than contribute to the stability of this new domain, lessens its willingness to constrain its own capabilities and operations in accordance with future cyber rules.

Although it will remain difficult to assess the credibility of any peacetime cyber commitments, the PLA's evolving strategic thinking on the topic could be a critical indicator of how Chinese cyber forces, under the aegis of the PLA's Strategic Support Force, China's new "information warfare service," might operate in an actual conflict scenario (*China Brief*, February 8). Looking forward, attempts to achieve consensus on these issues must take into account the PLA's concurrent advancement of strategic and doctrinal approaches to information operations, especially "cyber military struggle" (网络军事斗争), that include the PLA's conceptual integration of peacetime and wartime (平战结合); anticipated attacks against civilian targets, including critical infrastructure; the intended mobilization of civilian cyber forces, under the aegis of the concept of military-civil fusion (军民融合); and also the potential for a preemptive cyber attack, given the PLA's consistent "first strike" (先发制人) approach to information and cyber warfare. **[5]** These established aspects of the PLA's existing strategic thinking call into question the viability of negotiating norms that would have to supersede theories and practices that might already be incorporated into official strategy and doctrine. Despite such potential obstacles, the PLA's apparent interest in options for cyber arms control—against the backdrop of an intensified awareness of China's own vulnerability and superior U.S. offensive cyber capabilities—could nonetheless reinforce the incentives for its acceptance of an eventual agreement for cyber rules of the road.

A "Chess Game" of Cyber Rules?

Certain authoritative PLA strategists tend to view the formation of rules for the cyber domain predominantly in terms of great powers' strategic competition. General Hao Yeli, vice president of the China Institute for Innovation and Development Strategy and formerly deputy director of the Fourth Department (4PLA) of the General Staff Department (总参四部), argues that "the formulation of rules for cyberspace is actually just a process of great powers playing a chess game of interests" (*Global Times*, December 12, 2015). Similarly, Major General Ye Zheng, an influential Chinese information warfare theorist affiliated with the AMS Operational Theory and Regulations Research Department (作战理论和条令研究部), which is involved in the formulation of official PLA doctrine, has described the development of cyber rules as a "cyberspace strategic game and security struggle," especially in the case of rules regarding cyberspace management, usage, arms control, and conflict. **[6]**

This realpolitik perspective on cyber rules contributes to skepticism of U.S. intentions in efforts to formulate international cyber norms and an argument for advancing instead a distinctly Chinese agenda, centered upon the concept of cyber sovereignty. From Ye Zheng's perspective, the U.S. "has a double standard" in the development of cyber rules, since it seeks to 'seeks to impose a norm upon other countries but not upon itself,' especially with regard to cyber arms control. **[7]** In particular, Ye Zheng urges opposition to the U.S. agenda for cyber norms and the advancement instead of norms that are favorable to the "fulfillment of national cyber sovereignty." The PLA's intensified focus upon the defense of China's national cyber sovereignty has corresponded with diplomatic efforts, notably by China's cyber czar, Lu Wei, to advance international acceptance of a more expansive understanding of the concept. Given the high-level focus on cyber sovereignty—including Xi's frequently quoted remark that "cyber sovereignty is national sovereignty"—this could prove to be a *sine qua non* for Beijing. Although this outlook could constrain cooperation, even such "cyber realists" seem to recognize the necessity of a more secure cyber order and could be willing to compromise in order to achieve it. **[8]** For instance, Ye Zheng has suggested, with a cautious optimism, "It is possible that some cyber arms control agreements will be formulated akin to nuclear arms control and that they will lock up the "Pandora's box" of cyber warfare." **[9]**

Cyber Arms Control?

Although the PLA literature on the concept of "cyber arms control" remains relatively nascent, the initial analyses of the issue, including in *China Military Science* (中国军事科学), the AMS' official journal, suggest that this topic is starting to receive substantive consideration within the PLA. In particular, Lieutenant Colonel Lu Jinghua, a post-doctoral researcher at the PLA's AMS China-U.S. Defense Relations Research Center, has published several articles on cyber arms control, including an analysis of the divergences and opportunities for cooperation between the U.S. and China in this context. Although these articles represent the views of a relatively junior scholar within AMS, Lu, whose dissertation focused on U.S. strategic thinking on cyber warfare, appears to be one of the PLA's emerging experts on cyber conflict. **[10]**

While this particular perspective is probably not representative of a mainstream view at this point, such early examinations of the prospects for cyber arms control indicate an interest in and potential openness to options for constraining the use of offensive cyber capabilities. For instance, despite recognizing the difficulty of reconciling certain bilateral disagreements, Lu Jinghua evidently sees the need for some form of cyber arms control and is well versed in the relevant U.S. and international efforts. From Lu's perspective, the differences of opinion between the U.S. and China on this topic include the U.S. preference to apply existing legal and normative frameworks, including the Laws of Armed Conflict, to cyberspace, relative to China's preference for a new treaty and rules for cyberspace; the U.S. concept of "cyber security" in tension with China's focus on "information security" (信息安全), the latter of which implies more expansive control over information; and whether to "comprehensively prohibit" cyber weapons, a position for which Beijing has argued (even while likely advancing its own offensive cyber capabilities in practice), or only "partially prohibit" cyber weapons, based on the U.S. preference. Her recommendations for progressing toward cooperation on this issue include the development of a common understanding of basic terms and concepts (e.g., how to define a "cyber weapon"), the establishment of a cooperative mechanism to remove barriers to verification in a potential arms control scenario, and the creation of a norm regarding the usage of cyber weapons, since preventing their 'proliferation' is infeasible. In particular, Lu notes that the potential of efforts to build upon a common interest in constraining the use of cyber weapons and the existing initiatives in this area, such as the Tallinn Manual, which, as she notes, includes a form of cyber sovereignty as a basis for the application of existing international law to cyber conflict. She argues that the U.S. and China can use the regulation of cyber military operations as the starting point for more expansive cooperation on cyber arms control.

The emergence of such a range of views is perhaps an encouraging sign that U.S. discourse and diplomacy regarding cyber norms and the need for rules of the road are starting to have an attentive and, in some cases, reasonably receptive audience within the PLA. For instance, Lu Jinghua seems to be among what has been characterized as a cyber 'institutionalist' school of thought within the PLA, relative to the more realist perspectives of Hao Yeli, Ye Zheng, and others. Potentially, continued bilateral engagement on cyber issues, especially if inclusive of relevant stakeholders from the PLA, could be constructive. However, such theoretical arguments for cyber arms control currently come into tension with the PLA's prevailing strategic and doctrinal approaches to cyber warfare, which could supersede peacetime commitments.

Complications Based on the PLA's Strategic Thinking

Based on authoritative texts, certain aspects of the PLA's strategic thinking on and articulated operational approach to cyber warfare could complicate and would undermine the credibility of diplomatic commitments to even the most fundamental rules of the road for the cyber domain. Consistently, the PLA's approach to information warfare, which encompasses cyber warfare, has been characterized by the concept of "the integration of peace and warfare" (平战结合) and a corresponding lack of differentiation between civilian and military targets. According to the 2013 AMS edition of *The Science of Military Strategy* (SMS), "cyber attack and defense countermeasures are an everyday occurrence," such that cyber military struggle is underway "at all times," including anticipated attacks on civilian targets and critical infrastructure, such as power, transportation, and communications systems. **[11]** Similarly, by Ye Zheng's assessment, "The strategic game in cyberspace is not limited by space and time, does not differentiate between peacetime and wartime, [and] does not have a front line and home-front…" **[12]**

This highly integrated approach extends to the PLA's conceptualization of the forces that would participate in cyber operations, which would further blur the conventional distinction between military and civilian domains. Beyond the longstanding linkage of information warfare to the traditional concept of people's warfare, relatively authoritative sources, such as a 2005 AMS study guide on information operations, also allude to the participation of civilians in information warfare, observing that "the boundaries between military personnel and common people and between civilian-use and military-use [technologies] have all become indistinct." **[13]** Notably, the 2013 AMS SMS and also the 2015 NDU SMS both allude directly to the participation of civilian cyber forces in a conflict scenario. The AMS SMS argues, since "military and civilian attacks are hard to distinguish," the PLA should "persist in the integration of peace and war [and] the integration of the military and civilians," such that "in peacetime, civilians hide the military, [while] in wartime, the military and the people, hands joined, attack together…" **[14]** This intended participation of civilian forces—including relevant personnel from government ministries, civilian industry, and even "some non-professional hobbyists who possess specialized skills"—is often linked to the expansive concept of military-civil fusion. **[15]** Such mobilization of civilian forces is unorthodox relative to most Western militaries and could complicate attribution efforts in a crisis through enabling plausible deniability to engage in proscribed cyber activities.

In practice, those theoretical aspects of the PLA's approach to cyber warfare could translate into a focus on extensive peacetime "cyber preparation of the battlefield," which could undermine strategic stability. The PLA appears to take a highly integrated conceptual and likely operational approach to cyber reconnaissance (网络侦察) and cyber attack, unlike the U.S., which is legally required to maintain a distinction between Title 10 and Title 50 authorities in cyber operations. That is, for the PLA peacetime cyber reconnaissance (often characterized as cyber espionage) is considered "generally just the preparation for probable future cyber attack operations," since "cyber reconnaissance very easily transforms into cyberspace attack," if one only 'presses a button.' **[16]** For instance, even the code for Chinese "cyber weapons" used in espionage and offensive operations doesn't differentiate clearly between reconnaissance and offensive functions; rather, those functions often tend to be integrated within a single cyber "tool." (Belfer Center, February 4). Similarly, the 2015 NDU edition of SMS, presents the concept of "integrated reconnaissance, attack, and defense" (侦攻防一体), implying that the operational activities of Chinese cyber forces would likely take a less differentiated approach to these activities, which are inherently interrelated at the technical level. **[17]** Such operational integration, even if not directly proscribed by existing and nascent legal and normative frameworks, could raise the risks of misperception or misattribution of intent in a crisis scenario, given the lack of technical differentiation between ordinary cyber espionage and cyber preparation of the battlefield.

These consistent aspects of the PLA's strategic and doctrinal approach, which date back to PLA's early literature on information warfare from the 1990s, could prove challenging to change credibly based on diplomatic commitments that are difficult to verify. Such texts' advocacy for a lack of differentiation between peacetime and wartime, attacks without discrimination between military and civilian targets, and the mobilization of civilian forces in wartime cyber operations are certainly not amenable to the preferred U.S. normative frameworks. If the potential immutability of these practices is taken into account, ongoing efforts to advance cyber rules and cyber arms control could perhaps focus even more narrowly on cyber rules for which there would be the highest degree of shared interest and mutual vulnerability.

Conclusion

Although the terms of a hypothetical cyber consensus might seem suboptimal to the U.S. and China alike, the stakes could be high enough to motivate continued progression toward a common understanding of at least minimal rules of the road for this new domain. For instance, the Xi-Obama joint pledge to refrain from "attacks" against "critical infrastructure" (a concept defined differently by the U.S. and Chinese governments) during "peacetime"—which leaves open the option of peacetime "reconnaissance" to prepare for preemptive attacks—might be reframed as an absolute prohibition against all forms of cyber operations against certain forms of critical infrastructure (e.g., civilian nuclear facilities) at any time, with violations to be investigated and appropriate countermeasures approved by an independent international panel of experts. **[18]** Future progression toward a more comprehensive framework for a new cyber order might also require that the U.S. eventually recognize, at least in a limited, legalistic sense, the relevance of cyber sovereignty. Ongoing Chinese efforts to advance its own version of "cyber sovereignty," which evidently includes its implementation of expansive controls over the freedom of expression and information, might make U.S. and Chinese approaches to this issue seem irreconcilable (*China Brief*, April 16, 2015). However, given that proposed legal frameworks, such as the Tallinn Manual, do recognize that national sovereignty has relevance in cyberspace, it seems that there might be space for a compromise in which the U.S. and China might each acknowledge that certain aspects of the traditional notion of sovereignty do apply, while the U.S. continues to oppose China's particular interpretation of the concept. **[19]**

Looking forward, "cyber anarchy" will continue to be "what states make of it," and certainly cyberspace has thus far remained a domain in which a high degree of international anarchy has prevailed. **[20]** While appreciable differences certainly do and will remain between U.S. and Chinese perspectives and preferences, the apparent progression in the views of PLA theorists toward a more widespread recognition that such cyber rules and even cyber arms control could be necessary to reduce the risks of conflict is notable, perhaps even encouraging. If the U.S. can credibly demonstrate that it is not advancing a "double standard" and would adhere to restraints upon certain of its own cyber activities, then it seems plausible that the PLA might eventually reciprocate and perhaps even be equally constrained by a compromise regarding cyber rules that it perceived as fair and balanced. However, unless there were evidence that the PLA's strategic thinking on cyber warfare were starting to recognize and incorporate such restraints, it will remain difficult to determine the relevance of any future diplomatic commitments. While an eventual U.S.-China agreement on cyber rules might seem infeasible at this point, past examples of China's "socialization"—including, for instance, into the international arms control regime or based on its engagement in international institutions—do provide precedents for a trajectory that perhaps could ultimately be achieved in this new domain as well. **[21]**

Elsa Kania is a recent graduate of Harvard College who is currently working as an analyst at Long Term Strategy Group.

1. NATO Cooperative Cyber Defense Center of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," August 31, 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html
2. However, the credibility of these commitments has already been questioned, given evidence of continuing, if perhaps somewhat reduced, Chinese commercial cyber espionage activities, as well as potential ongoing cyber preparation of the battlefield. See the recent FireEye report, "Red Line Drawn," June 20, 2016, for further details on the apparent trends in Chinese commercial cyber espionage.
3. Although "network" is the literal and perhaps more appropriate translation of 网络, I choose to use the translation "cyber" for the purposes of this article for clarity.
4. Hao Yeli [郝叶力], "Great Powers Cyber Strategic Game and China's Cyber Strong Country Strategy" [大国网络战略博弈与中国网络强国战略], *International Relations Research* [国际关系研究], 2015.

[5] See: Joe McReynolds, "China's Military Strategy for the Network Domain," Joe McReynolds (ed.), *China's Evolving Military Strategy*, Jamestown Foundation, April 2016, for more extensive discussion of the topic.

[6] Ye Zheng [叶征], "A Discussion of the Innate Characteristics, the Composition of Forces, and the Included Forms" [论网络空间战略博戏的本质特征, 力量构成与内容形势], *China Information Security* [中国信息安全], August 2014.

[7] Ibid.

[8] See: Joe McReynolds, "China's Military Strategy for the Network Domain" for the initial framing of this cyber/network realist and institutionalist distinction.

[9] Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond,"Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, 2015.

[10] 吕晶华 [Lu Jinghua], 网络军备控制:中美分歧与合作 [Cyber Arms Control: Divergences and Cooperation Between the U.S. and China], China Information Security [中国信息安全], September 2015;吕晶华 [Lu Jinghua],《美国网络空间战思想研究》[Research on U.S. Strategic Thinking on Cyber Warfare], 军事科学出版社 [China Military Science Press], 2014; e.g., 吕晶华 [Lu Jinghua], 《国际网络军控问题研究》[A Study of International Arms Control in Cyberspace], 中国军事科学 [China Military Science], 2014.

[11] Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学]. Military Science Press [军事科学出版社], 2013.

[12] Ye Zheng [叶征], "A Discussion of the Innate Characteristics, the Composition of Forces, and the Included Forms" [论网络空间战略博戏的本质特征, 力量构成与内容形势].

[13] Xu Genchu [徐根初], eds., *Study Guide on Theories of Information Operations* [信息化作战理论学习指南], Military Science Press [军事科学出版社], 2005.

[14] Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学].

[15] Xu Genchu [徐根初], eds., *Study Guide on Theories of Information Operations* [信息化作战理论学习指南], Military Science Press [军事科学出版社], 2005.

[16] Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学].

[17] Xiao Tianliang [肖天亮], eds., *The Science of Military Strategy* [战略学]. National Defense University Press [国防大学出版社]. 2015.

[18] The proscription against the targeting of civilian nuclear assets with offensive cyber capabilities was previously proposed in the report: East West Institute, "A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets," January 2014.

[19] NATO Cooperative Cyber Defense Center of Excellence, "Tallinn Manual on the International Law Applicable to Cyber Warfare," 2013, https://ccdcoe.org/research.html.

[20] Alexander Wendt, "Anarchy is what states make of it: the social construction of power politics," *International Organization*, 46, no. 02 (1992): pp. 391–425.

[21] e.g., Evan S. Medeiros, *Reluctant Restraint: The Evolution of China's Nonproliferation Policies and Practices, 1980–2004*. NUS Press, 2009. Alastair Iain Johnston, *Social States: China in International Institutions, 1980–2000*, Princeton University Press, 2014.

*** *** ***

China Brief is a bi-weekly journal of information and analysis covering Greater China in Eurasia.

China Brief is a publication of The Jamestown Foundation, a private non-profit organization based in Washington D.C. and is edited by Peter Wood.

The opinions expressed in China Brief are solely those of the authors, and do not necessarily reflect the views of The Jamestown Foundation.

For comments and questions about China Brief, please contact us at wood@jamestown.org