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

VOLUME XV • ISSUE 8 • APRIL 17, 2015

In This Issue:

Lu Wei, the head of the State Internet Information Office.

(Source: Xinhua)

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 Nathan Beauchamp-Mustafaga.

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

1111 16th St. NW, Suite 320
Washington, DC 20036

Tel: 202.483.8888
Fax: 202.483.8337

In a Fortnight

ROLLING OUT THE NEW SILK ROAD: RAILROADS UNDERGIRD BEIJING'S STRATEGY

By Nathan Beauchamp-Mustafaga

The much-heralded arrival of the *Yixinou* train in Madrid last December, after traveling 8,000 miles from Yiwu, China, encapsulated the rapid expansion of China's railway network across Eurasia and the key role that railroads are playing in Beijing's New Silk Road strategy (Xinhua, December 9, 2014).

China's domestic railway infrastructure development is now often cast in the light of facilitating China's physical links with countries along the 21st Century Maritime Silk Road (MSR) and Silk Road Economic Belt (SREB), also known as the "One Belt, One Road." When three new railway lines—Lanzhou to Urumqi, Guiyang to Guangzhou and Nanning to Guangzhou—opened in late December, Xinhua said that "the completion of these railroads not only expands China's railway track another 3,000 kilometers, but also facilitates the main blood vessels

of the One Belt, One Road" (Xinhua, December 27). The Lanzhou to Urumqi line is "on the Eurasian bridge hinterland and goes through the core area of the Silk Road Economic Belt that the country is building," and will support development of China's western provinces, industrialization as well as connect Xinjiang with Central Asia and Europe.

A key component of China building railroads along the New Silk Road is the Chinese state-owned enterprises (SOEs) that stand to benefit considerably from their integral role in the initiative—China North Railway (CNR) and China South Railway (CSR), which are soon to merge (see *China Brief*, April 3). Premier Li Keqiang has championed them on his recent travels abroad as part of the government's "going out" strategy, touting them in Thailand, Eastern Europe and Africa, once telling China South Railways employees that "wherever I go, I promote China South Railways there!" (*China Youth Daily*, April 7). The state-run *People's Daily* wrote that the New Silk Road is "a road of cooperation, a road of peace, a road of mutual benefit and should become a paradise for Chinese multinational companies to pursue virtuous development" (*People's Daily*, January 26). Another newspaper said railroads have become China's "diplomatic calling card" and represent China's economic transition from manufacturing to innovation (*China Youth Daily*, April 7). The New Silk Road has also given CSR new business opportunities in Kazakhstan, Turkey, Thailand and the Balkans (see *China Brief*, October 23, 2014).

China has leveraged its railroad technology to further larger economic cooperation as part of China's outreach for the New Silk Road, especially with Russia. Foreign Minister Wang Yi, speaking at this year's National People's Congress, said the bilateral "win-win" relationship with Russia includes cooperation on the SREB and "promoting cooperation on building railways" (*People's Daily*, March 9). Stretching the definition of the New Silk Road, *People's Daily* said that "building the Moscow-Beijing pan-Eurasian high-speed rail is the leading direction of bilateral cooperation in core fields," and this applies to the Moscow-Kazan high-speed rail, which will "create a new freight hub in the Far East" (*People's Daily*, March 7; Russia Today, March 30). Chinese media have linked this cooperation to the fact that China's northeast will be tied to Russia's Far East through a railroad crossing Liaoning, Jilin and Heilongjiang provinces. This intimate relationship between the New Silk Road and Chinese railroad technology is also evident in Chinese companies building Turkey's new rail line between Istanbul and Ankara. In its coverage, *People's Daily* quoted a Turkish official voicing support for the New Silk Road and saying, "the One Belt, One Road strategy promoted by China coincidently matches up with Turkey's Four East Railways plan" (*People's Daily*, September 22, 2014).

Any military implications of China's outstretching railroad network are very likely to be confined to China's own territory. While China's domestic railways can certainly facilitate troop and mobile missile movements within the country and are likely designed with some level of military strategy in mind, railroads would likely only be useful if China had the cooperation of countries along the route—in the event of a war, other countries could easily bomb rail lines along the border (see *China Brief*, March 25, 2011). The PLA's interest in railroads is evident in a recent article in a military newspaper, which quoted a PLA expert as saying that Russia lost the Crimea War and Russo-Japanese War, over a century ago, due to "railway construction delays and misfortune" (*China National Defense Daily*, October 9, 2014). The expert added that with China's large land mass, railroads can be a "fast and effective" means for military deployments. The cooperation necessary for external movement was true in 2007, when the People's Liberation Army participated in the Shanghai Cooperation Organization's (SCO) "Peace Mission 2007" exercise after transporting some troops to Russia via rail, repeating this in 2010 and welcoming foreign troops via rail in 2014 (*PLA Daily*, July 27, 2007; Xinhua, September 22, 2010; Ministry of National Defense, July 31, 2014). Beyond being a relatively soft target, the main railway for the Silk Road Economic Belt has three different gauges of track between Yiwu and Madrid, requiring cars to be transferred each time (*China Daily*, July 19, 2013). This, however, has not stopped some countries from worrying about China's railways, as Vietnam in 2010 reportedly rejected a Chinese proposal to build a rail line, in favor of a Japanese plan, due to fears that China would invade using the connecting railroad (Xilu, November 24, 2010).

Railroads also play a crucial role in the New Silk Road's geostrategic significance. According to Shi Qiping, a Taiwanese scholar whose comments were later plagiarized by Xinhua, railroads support China's "counter-containment" strategy (Phoenix TV, December 19; Xinhua, April 1). Describing the political "new normal" of U.S. "repression, containment and encirclement," Shi said that by building railroads across Eurasia, China can move the economic center of gravity toward Asia, and "the United States will suddenly realize, originally we [the United States] were trying to contain you, but now you [China] are containing us." Xinhua made these comments more explicit by saying that the MSR will allow China to "break through the first island china to the east and enter the Pacific Ocean," "control the South China Seas to the south," and "enter the Indian Ocean from the South China Seas through the Malacca Strait," while the SREB is intended to break through U.S. encirclement. PLA Major General Ji Mingkui, a frequent military commentator on the New Silk Road, also touted China's railway cooperation with Thailand as a way to limit Japan's influence in Southeast Asia (see *China Brief*, February 20; China.org, December 12, 2014; China.org, December 24, 2014). Moreover, China and Russia are reportedly competing for influence in Central Asia in part over the railroad gauge to be used by those states—with China's loans likely predicated on using China's standard gauge (Author's interview, April 16).

Although the main thrust has been via the SREB to Central Asia and on to Europe, the Maritime Silk Road also utilizes railroads as part of its transportation network, as the two new rail lines to Guangzhou link China's southwest region to the ocean (Xinhua, December 27, 2014). The MSR route includes a railway from Kunming to Singapore, traversing Vietnam, Burma, Cambodia, Laos, Thailand and Malaysia (China Military Online, February 15). Mirroring the state-centric approach that has tied railroad SOEs to the New Silk Road along the SREB, one newspaper said that all countries in Association of Southeast Asian Nations (ASEAN) want railroads, but many have problems securing financing, and China's $40 billion Silk Road Fund is intended to solve this challenge—and in doing so create more opportunities throughout Asia that China no doubt will tie into its overarching strategic transportation strategy (China Military Online, February 15).

Although the Chinese government has been keen to export its railway technology since the mid-2000s, the New Silk Road provides an excellent framework to promote CNR and CSR abroad while also tying countries along the route together through physical infrastructure that will support China's future economic development, especially in its poorer border regions.

Nathan Beauchamp-Mustafaga is the Editor-in-Chief of China Brief.

***

China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy

By Joe McReynolds

When tracking the development of China's military capabilities, Western People's Liberation Army (PLA) watchers encounter frequent challenges in determining which data sources they should draw upon for their analysis. Purely quantitative measurements of the PLA's nominal force strength, though often valuable, may not provide insights into challenges the PLA faces in the real-world execution of its missions, while writings on Chinese military strategy by any given PLA author may not reflect the PLA's broader institutional stance or limitations imposed by inadequate material capabilities.

If one analyzes China's approach to network warfare in particular, these challenges are multiplied. **[1]** "Cyber weapons" are not publicly viewable and quantifiable in the same sense as submarines or aircraft, and often the PLA will not admit even their existence. And just as in U.S. discussions of "cyber war," charlatans and self-promoters abound; although it is easy to find writings by PLA officers theorizing loosely and grandiosely about information warfare, they are often speaking only for themselves rather than for their respective military institutions.

Roughly once every 15 years or so, however, the PLA's influential Academy of Military Sciences (AMS) issues a new edition of *The Science of Military Strategy* (*SMS*), a comprehensive, generally authoritative study of the PLA's evolving strategic thought that escapes much (though not all) of the shortcomings of other PLA original sources. The AMS plays a much more central role in the formation

of China's military strategic thought than its academic counterparts in the United States, and the *SMS* is its flagship external product. It is the result of dozens of high-level PLA authors working together over a period of years to produce a heavily vetted consensus document.

As a result, each new edition of the *SMS* is closely scrutinized by China hands in the West for the valuable insights it provides into the evolving thinking of the PLA on a range of strategically important topics. The newest edition of the Science of Military Strategy has recently been released, with Western PLA analysts beginning to obtain copies since summer 2014. Although no English translation is currently available, a book forthcoming this year from The Jamestown Foundation, *China's Evolving Military Strategy*, will aim to convey the central insights contained within this important new document to Western policy and analysis audiences.

The *SMS* is a particularly valuable resource for understanding China's evolving strategic approach to network warfare. A study that aims to be as comprehensive as the *SMS* cannot afford to ignore network warfare due to the centrality of information warfare to modern war-fighting, and the process by which the *SMS* is written ensures that the information analysts receive on network warfare represents something approaching an authoritative consensus within the PLA. The following are the most important revelations from the new *SMS* on the PLA's approach to network warfare:

The Fig Leaf is Gone: China's Network Warfare Forces Are Now Explicitly Acknowledged

In recent years, official PLA publications have repeatedly issued blanket denials of offensive activities in the network domain, such as that "the Chinese military has never supported any hacker attack or hacking activities" (China Armed Forces / 中国军队, No. 20, 2013) even as the evidence conclusively attributing various large-scale cyber intrusions to China has continued to mount. The release of the new *SMS* removes that barest fig leaf of plausible deniability. The *SMS* not only explicitly acknowledges that China has built up network attack forces, but divides them into three types:

- The PLA's "specialized military network warfare forces" (军队专业网络战力量), which are military operational units specially employed for carrying out network attack and defense

- "PLA-authorized forces" (授权力量), which are teams of network warfare specialists in civilian organizations such as the Ministry of State Security (MSS), the Ministry of Public Security (MPS) and others that have been authorized by the military to carry out network warfare operations

- "Non-governmental forces" (民间力量), which are external entities that spontaneously engage in network attack and defense, but can be organized and mobilized for network warfare operations

This is the first time an explicit acknowledgement was made of the existence of China's secretive network attack forces from the Chinese side, and it is particularly noteworthy that this acknowledgement extends beyond the military domain and into the network warfare capabilities of civilian government agencies. The AMS's statement that China's civilian network attack forces operate under the PLA's "authorization" may speak to an ongoing power struggle within the Chinese system between the PLA's leadership and the aforementioned civilian government organs to determine who truly oversees Chinese actions in cyberspace; as unprecedented as it is to have the Chinese military acknowledge the existence of its network attack forces, having a PLA publication be the first to announce the existence of such secretive forces inside the civilian government is particularly unusual, and may represent an attempt to "plant the flag" for the PLA.

This could also seriously complicate China's international efforts at law enforcement cooperation on cybercrime. The MPS, which is more or less "China's FBI," has assisted more than 50 countries in investigating over a thousand cases of cyber-crime in the past decade, and China has established bilateral law enforcement cooperation with over 30 countries (including the United States, the United Kingdom, Germany and Russia), often including a cyber-crime component (China Armed Forces, 2013). With the Chinese now explicitly acknowledging that the MPS has

network warfare forces stationed within it, the United States and other targets of Chinese state-sponsored hacking will have to weigh carefully whether cooperation with the MPS on cyber-crime is worth the risks.

Blurring the Divide Between the Military and Civilian Realms

In keeping with Chinese President Xi Jinping's recent statements that "without network security there is no national security" (PLA Daily, October 7, 2014), the authors of the new *SMS* break from the previous edition's vague talk of overall information warfare objectives to concretely assert the centrality of cyberspace power to China's overall ability to project national power, engage in strategic deterrence, and defend itself in a conflict. However, this "network domain," which has become so central to the PLA's warfighting, exists primarily as civilian infrastructure and is used globally for civilian purposes. As a result, although development of elite network warfare personnel remains central to the PLA's ongoing cyber mission, the authors of the *SMS* focus an unusual amount of their energies examining the importance of civilian information technology and the civilian Internet to network warfare.

First and foremost, the authors believe that civilian infrastructure in foreign countries can be targeted more freely with network warfare than with conventional weapons, without provoking the degree of conflict escalation that a conventional attack on civilian targets would. This echoes an idea known as "unrestricted network warfare" (网络超限战) long advocated by some of the PLA's more hawkish network warfare theorists, and its presence in an authoritative work such as the *SMS* suggests that more aggressive voices may be gaining ground in the PLA's internal deliberations on network warfare strategy (See Dong Qingling and Dai Changzheng, "Deterrence in the Network Space: Is Retaliation Feasible?"). To put it simply, they believe that the old playground sports adage of "no blood, no foul" applies to network warfare, even if the attack in question has debilitating effects on civilian infrastructure, and in a conflict scenario they may advocate that the PLA chooses its targets accordingly.

Second, the authors of the *SMS* acknowledge that China's civilian information technology (IT) industry functions as a core component of China's overall power in cyberspace. Since the development of China's network warfare capabilities relies heavily on human talent and the civilian IT industry is where the bulk of China's IT talent is found, PLA analysts believe that civilian industry will continue to serve as an important source of technical talent and human capital for the PLA's network warfare operations to a degree that is disproportionate to the PLA's reliance on civilian industry in other realms of warfare. The authors also emphasize the fact that despite recent advances in Chinese IT, key state-of-the-art networking technologies are still advanced primarily in the West, and the bulk of the Internet's core architecture is controlled by the United States and its allies. Thus, what the West views as the neutral "status quo" of the network domain is, to China, an intolerable "network hegemony" (网络霸权) imposed by the United States and others. Based on the increasing prominence of these sentiments within the PLA, the prediction one sometimes hears in the West—that China's IT development will one day transform it into a "mature" partner interested primarily in cyberspace cooperation to preserve our "mutual" interests—appears likely be overly optimistic. The PLA's stated intentions to mobilize its civilian IT industry as a component of national power in both peacetime and wartime must be accounted for in the calculus of determining whether any given Sino-U.S. information security cooperation is in the United States' national interest.

"Salami-Slicing" in Cyberspace and Planning for Resilience in the Face of the Inevitable

The *SMS* authors also focus heavily on the central role of peacetime "network reconnaissance"—that is, the technical penetration and monitoring of an adversary's networks—in developing the PLA's ability to engage in wartime network operations. As the *SMS* puts it, since the technical principles underlying successful penetrations of an adversary's systems are essentially the same whether the objective is reconnaissance or active disruption, at the appropriate moment "one need only press a button" to switch from reconnaissance to attack.

Despite this ambiguity of intent, since network reconnaissance is both non-destructive (at least initially) and widely engaged in by all nations for the purposes of espionage, the *SMS* authors believe it has been clearly demonstrated that the act of network reconnaissance

alone is unlikely to lead to escalation or the outbreak of war. As a result, PLA strategists appear to have arrived at a strategic understanding of peacetime network operations similar to China's "salami slicing" tactics for asserting control of disputed islands in the South China Sea: a pattern of taking actions during peacetime that incrementally put China into a superior tactical position should conflict ever break out but that, which while provocative and unwelcomed by China's neighbors, are unlikely to lead to direct conflict in and of themselves. If conflict eventually does break out, China will be in a better position than they otherwise would; if it does not, they will have incrementally gained much of what they desire without a fight.

PLA analysts understand, however, that network reconnaissance is not by any means one-sided, and believe that just as they are actively attempting to penetrate the networks of their adversaries, the PLA's networks are likely being repeatedly breached as well. Furthermore, they argue that since China's "main strategic opponent" (their euphemistic way of referring to the United States) has superior network warfare capabilities, the strict balance of power in a network-domain conflict would not necessarily tilt in China's favor. As a result, the *SMS* emphasizes that the PLA must plan for a future of network warfare in which its defenses will inevitably be breached, military networks will at times be taken down by hostile adversaries, and China's modernized C4ISR systems cannot be fully relied upon. **[2]** Although they do call for a major effort to strengthen China's network defenses, this is undertaken in the hope that those defenses will not catastrophically fail, without any expectation that they will fully withstand outside attacks.

For Western military analysts, this line of thinking should trigger particular attention and concern. With China preparing for conflict in the network domain under the assumption that from the outset their information networks will quickly be heavily degraded and only partially functional, there will be a strong incentive in a conflict for the PLA to push the envelope of what is globally considered legitimate in areas such as anti-satellite warfare. The intersection of U.S. technological reliance on space-based C4ISR systems with its distance from East Asia will multiply this incentive, as China will (all other things equal) be able to do "more with less" in its immediate backyard.

Much of the focus by Western analysts when examining China's approach to anti-access/area-denial (A2/AD), also known as "counter-intervention," has centered on the physical realm of warfare, including the use of precision-guided munitions reliant on C4ISR. However, as the insights contained in the new *SMS* demonstrate, this discussion is fundamentally incomplete if it does not take into account China's evolving approach to network and information warfare. Rightly or wrongly, many Chinese analysts believe that the United States currently possesses what they term a "no satellites, no fight" military force, and in a major conflict scenario they appear increasingly likely to put that presumption to the test.

Joe McReynolds is a Research Analyst at Defense Group Inc.'s Center for Intelligence Research and Analysis. His research interests primarily center on China's approach to computer network warfare and defense science & technology development. Mr. McReynolds has previously worked with the Council on Foreign Relations and the Pacific Council for International Policy, and is a graduate of Georgetown University's School of Foreign Service and Graduate Security Studies programs. He speaks and reads Chinese and Japanese, and has lived and studied in Nagoya, Guilin and Beijing.

Notes

1. Rather than mirroring the United States' 'cyber' concept, PLA writing speaks at the broadest level of the 'information domain' and 'information warfare,' with network, electromagnetic, psychological, and intelligence warfare each taking place as distinct components of that broader concept. The PLA concept of "network warfare" is roughly analogous to the current United States cyber concept, though not always identical in its details.

2. C4ISR stands for command, control, computers, communication, intelligence, reconnaissance and surveillance.

***

China's Maodun: A Free Internet Caged by the Chinese Communist Party

By Amy Chang

China pursues a strategy of aggressive cyberspace management and is in the midst of fostering a military cyber force to further the Chinese Communist Party's (CCP) primary interest: to stay in power. Secondary considerations that directly or indirectly support the continuation of CCP rule include the preparation for military conflict, the sustainment of economic growth, the control of content and of expression online as well as the reinterpretation of what it means for a country to manage the Internet. **[1]**

The Chinese leadership has recognized that the proliferation of information technology has the potential to enhance economic output in a globalized world, though they also recognize that it also has the potential to undermine CCP rule. China now has the largest online population in the world, which is now surpassing 649 million users, though close to half of its population is still without access to the Internet (Cyberspace Administration of China, February 3) While the Chinese government wants to help its citizens get online to foster economic growth and stability, it also wants to be able to steer discourse toward "rational use of technology" and limit accessible information to maintain political legitimacy (State Council Information Office, June 8, 2010). This need for control manifests in China's cybersecurity strategy.

You Say "Cyber," I Say "Network"

The divergent use of terminology for cybersecurity between Western states and China is important to delineate. The Chinese concept for "cybersecurity" is understood as "network security," (*wangluo anquan*) couched under the umbrella term of "information security" (*xinxi anquan*), and includes the "use of information…to influence or control the direction of an opponent's decision-making activities." **[2]** Unlike the more direct and limited scope of the term "cybersecurity" used in the West to concern the "ability to protect or defend the use of cyberspace from cyber attacks," the use of the term "network security" in China implies that it conceives of network security to have national security implications—and hence, economic, political and social components (NIST, Glossary of Key Information Security Terms; Xinhua, February 27, 2014).

Objective: Secure CCP Rule

The most important goal for China is to maintain CCP control: without power and the projection of legitimacy to its population, they would not be able to govern. Their cybersecurity strategy is derived from this main driver. Other manifestations of China's cybersecurity strategy include: maintaining economic growth and stability, which involves industrial economic cyber espionage of foreign targets; protecting the governing power of the CCP through information control, propaganda and targeting of domestic sources of potential unrest; preparing for military scenarios and ensuring military superiority in the event of cyber conflict with an adversary through military modernization, computer network operations research and human capital cultivation; and advancing alternative narratives of government control over/handling of cybersecurity internationally (e.g., promoting sovereignty of states to control the Internet within a country's borders) and domestically (e.g., justifying domestic surveillance, information control).

Economic growth is a secondary consideration, but an essential component in keeping the CCP in power. To the central leadership, providing consistent improvement in the livelihoods of the Chinese population is essential. In order to facilitate that growth, the Chinese government conducts or commissions state-sponsored entities to exploit the cyber domain as a vehicle to obtain valuable information for economic gain. Chinese actors or state-sponsored actors ex-filtrate the intellectual property of foreign companies. Industrial cyber espionage, where countries and non-state actors exfiltrate large amounts of industrial economic information including trade secrets, research and development as well as products, occurs at a massive scale in China. While many U.S. and Western analysts and significant public attention focus on this aspect, they must remember the broader motivating factors beyond their immediate economic or security impact.

Political control is a necessary factor in China's cybersecurity policy, and China also employs or sanctions cyber activity (e.g., limits to information access on the Internet and social media) in the name of protection of domestic political stability. The Chinese government targets "revisionist organizations," "separatists, extremists, splittists" and Western imperialist forces that aim to disrupt social stability. The government then screens the Internet and social media and promotes propaganda to counter these "forces" (Ministry of Foreign Affairs). For example, China has created the Great Firewall, an intricate system of Internet controls that filters out "harmful" domestic and foreign content and communications which, in practice, creates a Chinese intranet that connects to the greater Internet infrastructure through a cyber "demilitarized zone" complete with filters, deep packet inspections and other forms of "cyber border security." **[3]** The Chinese government worries that unrestricted Internet access or uncontrolled information might pose a significant risk to the Chinese communist regime's stability and hold on power.

An example where the Chinese government indirectly supports the control of information is through the social media platform WeChat. An amalgamation of Western equivalents for Facebook, Twitter, Instagram, WhatsApp and Venmo/PayPal, WeChat is a platform that has over 500 million active users worldwide, with the vast majority of active users located in China. As the Chinese government had made these distinct individual Western platforms nearly impossible to access in China (unless accessed through a Virtual Private Network, or VPN), Chinese web users are forced by limited options to use Chinese platforms—which are easily controlled by the Chinese government—over Western alternatives.

China has since strongly emphasized the importance of information and communications technology for the future of warfighting, aspiring to prevail in "local wars under informatized conditions by 2050" (Information Office of State Council, China's National Defense in 2006). Network operations "are expected to play an important role" in military scenarios involving Taiwan, other territorial or maritime conflicts, or the United States. **[4]** China also devotes significant effort in studying their political and military adversaries' military infrastructures, motivations, capabilities and limitations.

Chinese Leadership on Network Security and Internet Sovereignty

Two recent senior leader–level developments on network security are worthy of mention: the establishment of the National Security Commission in November 2013 and the formation of the Central Network Security Informatization Leading Small Group in February 2014. The National Security Commission underscored the importance of domestic security to the central government, as well as the government's inclusion of a broad swath of topic areas including network security (*People's Daily*, May 6, 2014) The Leading Small Group signaled a new, high-level prioritization of cyber as a major strategic initiative with political, economic and military implications and also indicated the relative importance of network security on the Chinese political agenda. Despite China's ongoing efforts to coordinate and organize the network security infrastructure, however, it remains fragmented, partly as a result of the disjointed state of the Chinese government's frequently overlapping and conflicting administrative bodies and managing organizations.

The CCP's self-preservation priorities guide the dominant political domestic narrative and drive its foreign policies and foreign cyber activity, all of which complicates the United States' and other countries' abilities to shape China's behavior in cyberspace. The Chinese government is attempting to alter how nations understand their role in Internet governance by advancing a concept called "Internet sovereignty." Internet sovereignty refers to the idea that a country has the right to control Internet activity within its own borders, and it is what China refers to as a natural extension of a nation-state's authority to handle its own domestic and foreign affairs (CPC News, July 22, 2014).

The movement is backed by Lu Wei, the head of the State Internet Information Office, the Cyberspace Administration of China and the director of a powerful cybersecurity strategy group comprised of China's top leaders. Lu's influence is backed by years of active Chinese promotion of Internet sovereignty in domestic propaganda efforts, government White Papers, Internet conferences, bilateral and multilateral meetings as well as United Nations meetings. China continues to engage the international community, wishing to signal to other

countries that it is a responsible and cooperative actor on technology issues. Understanding that international norms and law have yet to codify Internet governance and cyber activity, China has invested significant effort to set the course for international norms in Internet governance.

Two recent developments that support China's desire to control information and localize data are the consideration of the China Banking Regulatory Commission's (CBRC), National Development and Reform Commission (NDRC), Ministry of Science and Technology (MOST), and Ministry of Industry and Information Technology's (MIIT) new Guidance Opinion provisions on the use of foreign technology in China in September 2014 and the draft anti-terrorism law. The CBRC opinion would require that all technology used in China's banking industry be "secure and controllable," which would mean that foreign information technology firms would have to establish their own research and development centers in China, hand over intellectual property rights to Chinese institutions and file source codes with CBRC (CBRC, September 3, 2014). The anti-terrorism law would require similar actions as the CBRC regulation, but technology firms would also be required to install backdoors on information technology (IT) products, transfer encryption keys to the government, and maintain servers and store user data in China (*Caixin*, April 2).

Implications for China and Conclusion

While foreign nations, most notably the United States, continue efforts to persuade China to cease its activities in cyberspace that compromise U.S. interests, it is unlikely that China will heed to U.S. demands. China's motivations are internally derived, and primarily focused on regime stability. China will not alter its activity in cyberspace if risks remain low, benefits remain high, and if solutions threaten CCP rule, potentially introduce instability or impede on China's "core interests."

However, as China continues to expand its Internet population and continues to grow in economic and political influence, China will encounter serious challenges. First, there may be limitations of censorship and control over Internet content for a rapidly growing online population. The Chinese leadership will either have to innovate new methods for easy content control or dedicate substantially more resources to information control efforts. Second, as China's economy continues to grow, it will focus on improving domestic industry and company access to foreign markets. However, limiting access to foreign information in China's controlled Internet environment may limit the ability of Chinese companies to conduct international business or commerce. Additionally, China's internal cybersecurity may suffer from vulnerabilities from poor network security infrastructure, where pirated software and security loopholes wildly proliferate (as an example, experts estimate that over 80 percent of PCs running Microsoft Windows use pirated software). **[5]** The success of China's cybersecurity strategy and its version of Internet governance also depends on the level of coordination on cyber issues across civilian and military leaderships. Lastly, convincing the broader international community to sign on to China's version of Internet governance is, at the moment, an unappealing approach for many Western and developing countries. The road toward executing China's vision for a comprehensive cybersecurity strategy looks rough ahead, though the investment of time and a strong will may prove skeptics otherwise.

These views presented in this paper are my own and do not represent those of either Chairman Matt Salmon of the Asia and the Pacific Subcommittee or Chairman Ed Royce of the Foreign Affairs Committee, U.S. House of Representatives.

Amy Chang is the Asia and the Pacific Subcommittee Staff Director at the U.S. House of Representatives Committee on Foreign Affairs. Previously, she was the Norman R. Augustine Research Associate in the Technology & National Security Program at the Center for a New American Security (CNAS). Her research interests included U.S. national security strategy, cybersecurity, military technological innovation, U.S-China relations and Asia-Pacific security. Prior to joining CNAS, Ms. Chang has worked at Albright Stonebridge Group, Defense Group Inc., the U.S.-China Economic and Security Review Commission (USCC), Project 2049 Institute and the Council on Foreign Relations.

Notes

1. For a more comprehensive analysis of the CCP's cyber strategy, see: Amy Chang, *Warring State: China's Cybersecurity Strategy* (Center for a New American Security, December 3, 2014).

2. Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington: National Defense University Press, 2009).

3. For a more detailed examination of the Chinese government's Internet infrastructure and censorship system, see *Economist*, April 6, 2013.

4. William Hannis, James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (New York: Routledge, 2013): p. 221.

5. *Financial Times*, March 18.

***

Chinese Views on the Information "Center of Gravity": Space, Cyber and Electronic Warfare

By John Costello

This paper seeks to examine the intersection of Chinese thought on cyber, space and electronic warfare, particularly in the context of command, control, computers, communication, intelligence, reconnaissance and surveillance (C4ISR) complexes and their use in the current military paradigm. Space warfare is still in a fairly nascent phase of use, just as space is still in its early stages of development and use as a major resource for humanity. The use of military long-range communications systems and the proliferation of complex, layered networks separate from the Internet backbone have only complicated the strategic implications of disruption and denial.

The Internet "Embargo"

An Internet defined by geopolitical lines and "cyber borders" serves China's interests, both domestically and internationally. Establishing geopolitical boundaries is increasingly being viewed by regimes such as China, Russia and Iran as a mitigating step to subvert many of the strengths from the U.S.-dominated global Internet infrastructure. Tightening border security between national intranets and the wider global infrastructure will be a huge factor in these countries' defensive protection. Chinese domestic policy regarding Internet businesses and censorship has fostered a de facto protectionist e-commerce: Chinese companies are, by law, required to serve at the behest of government sensors and monitoring apparatuses. Western companies have been banned or, unwilling to comply, have been unable to gain a foothold in the market. This has created an almost entirely separate internal cyber environment, within China spurred on by the participation of nearly 650 million Internet users. Chinese e-commerce has developed to the point where it does not fundamentally need foreign participation, and maintains a healthy business environment in a nearly isolated and independent setting. The Internet in China could be called an almost entirely separate commercial ecosystem: an Internet autarchy.

Chinese commentators and theorists, including Major General Ye Zheng, an Academy of Military Science academician and influential information warfare expert, and to a lesser degree, Lu Wei, the head of the General Office of the Central Leading Group for Internet Security and Informatization, advocate for increased cyber border protection and defensive systems—if not to control internal dissent than to reduce foreign influence on the Chinese, a sort of "soft blockade" more akin to customs searches and seizures than a hard embargo (People's Daily Online, July 22, 2014; Huffington Post, December 15, 2014). The technologies advocated, though, would allow China, or any nation with a similar infrastructure, the capability to effect an Internet, or information, "embargo." As a defensive measure, any country that has created an Internet commerce system with a high degree of autarchy could execute this sort of hard Internet "embargo" without devastating loss.

This is a "nuclear" option, and war planners in China know that. Embargos, or their close cousin, economic sanctions, can be a *casus belli* for potentially aggressive states, escalate tensions or signal a forthcoming pre-emptive attack. Authoritative Chinese writings make clear that in a conflict scenario where hostilities are inevitable and both information and national security dispositions are strongly in China's favor, a pre-emptive network attack would be the first salvo in a conflict. **[1]** To ensure

complete cyber borders, China would erect a cyber "great wall" to diminish cyber cross-sections, vectors of attack and points of ingress into critical infrastructure, essentially embargoing incoming and outgoing data to minimize the risk of command and control (C2) implants or network sabotage. It would be likely that other countries, including the United States, would follow suit. It is unclear whether this would be accomplished by physical destruction of the greater Internet backbone, or strong firewalls, packet filtering and deep packet inspection.

Cyber Warfare: The "Nuclear Warfare" of the Information Era

With the rise of precision-guided munitions and the C4ISR complexes that enable them, modern warfare has undergone a transformative shift akin to the logistics innovations noted above. This shift toward extended communications lines, enabled by information networks and satellite assets, has made the principles of total war described by Carl von Clausewitz and Antoine-Henri Jomini extremely relevant today. Ye Zheng himself believes that what nuclear warfare was for the industrial era, cyber warfare will be for the information era. **[2]** This is not surprising. Nuclear warfare disrupted the concepts of strategic points, massive warfare formations and overwhelming force, upending the "total war" industrial mobilization that required an extensive and complex logistical network. Militaries of the world adapted, with logistics networks becoming streamlined to reduce exposure and platforms becoming more self-reliant and independent.

China's Calculus For a Pre-emptive Strike

According to authoritative Chinese sources, information warfare and in particular, cyber warfare, operate under similar principles. A preemptive first strike is preferable as it sets the stage for the remainder of the conflict and puts the aggressor in a distinct position of advantage. For nuclear and kinetic warfare this constant preparation *in* the battlespace translates into constant intelligence preparation *of* the battlespace. Chinese military strategists, in particular Major General Ye Zheng, have confirmed what Western analysts have suspected for a long-time: The PLA advocates a cyber-posture that makes no differentiation between peace-time and war-time, and, in fact, advocates for a state of perpetual mobilization. In his *Lectures on the Science of Information Operations*, Ye Zheng notes: "Information attack actions do not distinguish between wartime and peacetime." **[3]**

Secondly, Chinese strategy presupposes the use of a pre-emptive strike against a potential aggressor. As soon as cyber warfare becomes a reality in a conflict, potential avenues of attack close, enemy vulnerabilities are mitigated, defenses are drawn up and the covert and presumptive nature of secrecy that is take for granted in peace-time cannot be used as an advantage. The status quo changes and the power of cyber warfare over the Internet decreases considerably. The single greatest vector of attack is destroyed after the first salvos are fired, and the digital soldiers, scouts, spies and saboteurs are exposed or rendered irrelevant. With physical or network access limited by geopolitical borders, Internet embargos and increased cyber security under threat or reality of cyber-attack, the most promising avenue, then, is via the electromagnetic spectrum (for example, wireless radio) that connects these machines. In war-time, the Internet is no longer an option for cyber-attack. Information operations planners have to plan for a contingency where the electromagnetic spectrum is the only viable option.

The Electromagnetic Spectrum

The electromagnetic spectrum comprises all frequencies of all forms of electromagnetic radiation, which are used for communications, RADAR and optics, among others. It is the "air, land and sea" for extended communications, C4ISR complexes and information technology, forming the medium by which all electronic communication is transmitted. In the 2013 edition of *The Science of Military Strategy*, the editors and writers make clear that in Chinese strategic thought, the electromagnetic spectrum is a fundamental natural domain equivalent with the air, land and sea and they view its defense as a defense of national sovereignty. **[4]** Simply put, the electromagnetic spectrum must be corralled and defined by China's geopolitical borders. Its ubiquity and power to transcend national boundaries makes it a potential liability for a nation that heavily censors most forms of media. Both Lu Wei and Ye Zheng, leaders in political and military realms, respectively, tie cyber defense and cyber borders to national defense against threats both internal and external.

Space and the "Information Center of Gravity"

To crouch it in the "supply lines" and "logistics" terminology used earlier, space-based assets, such as satellites, act as crucial strategic relay points, fulfilling the same role in information "celestial lines of communication" as depots and way-points do for terrestrial "lanes of communication," namely trade, shipping and logistical supply.

The current military paradigm, of which the United States is the undisputed model, heavily relies on these space-based assets in order to wage war. Satellites are relays for long-range command and control. They transmit vital intelligence out of theaters of warfare to domestic intelligence processing facilities, planners and decision-makers. Some even act as strategic sensors, collecting and then transmitting intelligence to war-fighters and intelligence professionals alike.

These satellite assets have become integral parts of isolated battlefield networks and military intelligence networks. These are networks that are "air-gapped" and do not necessarily depend on wired communication for transmission but rather rely on a combination of heavy encryption and authentication measures transmitted over the electromagnetic spectrum to establish links with data nodes and users.

This extended enterprise of networked intelligent machines carrying vast amounts of information to tactical, operational and strategic users has fundamentally revolutionized warfare in what the Chinese would call the "Revolution in Military Affairs." This shift in extended information supply and C4ISR complexes enabled by space-based assets mirrors the industrial warfare logistical innovations from the 18th, 19th and 20th centuries. As logistical lines of supply would comprise the key points in their physical centers of gravity, the "celestial supply lines" of networked machines transmitted over the spectrum and relayed by space assets are the strategic nodes of the "information center of gravity." Major General Chang Xianqi, a professor at the Academy of Equipment and Command Technology, in his book *Military Astronautics*, further argues that the opening action of any future war will likely take place in space, due to its nature as a center of gravity. **[5]**

Space, Cyber and Electronic Warfare

The space-based assets that constitute the information center of gravity—those communications satellites and sensors—remain exclusively dependent on the electromagnetic spectrum. Electronic warfare exploits this key vulnerability and essentially affects a "blockade" of information, preventing receivers from being able to collect and process the intended signal.

Cyber warfare, limited in a war-time environment by "Internet embargos," can still be heavily utilized over the electromagnetic spectrum. The massive resources required to execute this type of attack successfully make it potentially prohibitively difficult. Maintaining the intelligence framework and manpower to ensure the continued viability of an attack is a costly concern. The intended target would have to be important enough that resources dedicated to disrupting it would be well spent. This rings true not just for China, but for any technological advanced nation with an eye for dominance in the space domain. As space assets serve as the backbone of the information center of gravity, they would be a primary focus in developing these type of cyber-electronic weapons.

National Defense University researchers Xiao Wenguang and Li Yuanlei explain that military satellites do not connect with the Internet backbone and remain independent and isolated battlefield networks. Hackers can still invade and disrupt a satellite network or take control of the telecommand of the satellite itself. Essentially, Xiao and Li believe that if military technology is sophisticated enough, one can use electronic warfare to deliver a cyber-attack over satellite communications, using it as a "springboard to invade the enemy's independent network systems." **[9]**

Evidence suggests that Chinese hackers have already conducted an attack on satellite systems similar to what is described above. In its 2011 report to Congress, the U.S.-China Economic and Security Review Commission (USCC) alleges that Chinese hackers were able to take control of two NASA satellites in 2011, Landsat-7 and Terra EOS AM-1 (U.S.-China Commission, November 2011). The report states that "each experienced at least two separate instances of interference apparently consistent with cyber activities against their command

and control systems." While the vector of attack was not one delivered via electronic warfare, it does highlight the fundamental threat of cyber-attacks against satellite command and control.

Major General Ye Zheng explains in his lectures series *Lectures on the Science of Information Operations* that technological convergence has increasingly made integrated network and electronic warfare weapons viable on the battlefield. The idea of isolated battlefield networks is becoming a relic of the past, as more and more sophisticated systems pervade modern warfare. Effecting a network "invasion" via injection of malware over the electromagnetic spectrum is a priority, despite serious technological barriers. **[10]** In the face of these barriers, a simple and brutish electronic "blockade" would suffice and, failing that, a kinetic strike would be the weapon of last resort. It would be simple, effective and have a high degree of expected success.

Conclusion

Satellites are the hallmarks of entrenched powers. The high-cost, technological development and human capital required to field them mandate that only a nation-state with a high degree of development, a successful economy, an inherent military or commercial need and unified political will can develop and deploy them. It is clear that as the developing nations of the world take ever greater steps upward, space will become a hotly contested environment. Chinese predictions of space being the stage for the opening shots in a future conflict will likely be judged prescient. Technological convergence and the slowly enveloping net of information carried by wires, radio and networks will continue to extend into space and wrap these expensive nodes into the greater global information infrastructure. But these costly and immediately outdated satellites are prohibitively expensive to replace and impossible to upgrade. Once in orbit, they cannot keep up with the ever increasing offensive capability of cyber and electronic attack. Once deployed, their operations are at the mercy of their vulnerabilities, whose discovery is often-times not a matter of "if" but a matter of "when."

The bloated and over-extended supply lines of industrial warfare were upended by the nuclear bomb. With the paradigm of military strategy disrupted by such a weapon, planners had to reckon with the new realities of a changing world. Supply lines were streamlined, overseas logistics bases were consolidated and strengthened and platforms were built to be larger and more self-sufficient. Strategically, the primary centers of gravity of military's around the world needed to shift. A similar transformation is happening today. Chinese strategists have laid out a clear understanding of the realities of the "information center of gravity" and the role that space, cyber and electronic warfare play. The warning is clear—the very enabling technologies of great military powers could well be their own undoing.

John Costello is a Research Analyst at Defense Group Inc. Prior to that he was a member of the US Navy and a DOD Analyst. He specializes in information warfare, electronic warfare and non-kinetic counterspace issues.

Notes

1. Ye Zheng, 信息作战学教程 [*Lectures on the Science of Information Operations*], Military Science Press, 2011, p. 45.
2. Ye Zheng and Zhao Baoxian, "关乎国家存亡：看网络战的五种作战样式" [A Matter of National Survival: Looking at the Five Forms of Combat in Cyber Warfare], June 3, 2011.
3. Ye Zheng, *Lectures on the Science of Information Operations*, p. 53.
4. Academy of Military Science Military Strategy Studies Department, 战略学（2013年版）[*Science of Military Strategy (2013 Edition)*], Military Science Press, 2013, p. 107.
5. Chang Xianqi, 军事航天学 [*Military Astronautics*], (Beijing: National Defense Industry Press, 2005), pp. 259–60.
6. Dai Qingmin, 网电一体战引论 [*An Introduction to the Theory of Integrated Network and Electronic Warfare*], Beijing: Liberation Army Press, 2002, p. 33; Ye Zheng, *Lectures on the Science of Information Operations*, pp. 44–45.
7. Qi Xianfeng, 空间信息系统防护探讨

["Discussions on the Protection of Space Information Systems"], 装备指挥技术学院学报 [Journal of the Academy of Equipment and Command Technology], 5 (2007).

8. Ye Zheng and Zhao Baoxian, "关乎国家存亡：看网络战的五种作战样式" [A Matter of National Survival: Looking at the Five Forms of Combat in Cyber Warfare], June 3, 2011.

9. Xiao Wenguang and Li Yuanli. "计算机网络与未来战争" [Computer Networks and Future Warfare], 江苏航空 [Jiangsu Aviation] 1(2007).

10. Ye Zheng, *Lectures on the Science of Information Operations*, pp. 91–94.

***

Chinese Military Think Tanks: "Chinese Characteristics" and the "Revolving Door"

By Silvia Menegazzi

Following Chinese President Xi Jinping's recent call on October 27, 2014 to build think tanks with "Chinese characteristics," growing attention has focused on the impact his remarks have had on think tanks in China dealing with foreign policy and economics (see *China Brief*, December 19, 2014; *Guangming Daily*, December, 25, 2014). The Chinese media has covered the domestic debate over this new approach to think tanks, with Chinese academics and policy analysts discussing the future trends and likely development path of think tanks, whereas, the foreign media has attempted to better understand the policy implications. Yet, few analyses have directly addressed how President Xi's proposal will impact other think tank sectors, most notably China's military think tanks. The announced reforms will likely stifle what was an increasingly free environment within PLA academic circles, at least at the public level, limiting the utility for Western officials and academics of interacting with these Chinese think tanks.

A Survey of Chinese Military Think Tanks

Focusing on the wider defense and security sector, there is a diverse array of think tanks that support the Chinese government and military's thinking and strategy on critical issues. Among the most prominent are: the Academy of Military Sciences (AMS), the Chinese Institute for International Strategic Studies (CIISS), the Center for Peace and Development Studies (CPDS), the Foundation for International Strategic Studies (FISS), the Institute for National Security Studies–National Defense University (INSS/NDU) and the China Defense Science Technology Information Center (CDSTIC). These think tanks usually interact with top leaders through closed meetings and internal reports. Moreover, through their close proximity to the PLA's core leadership, informal conversations with Chinese Communist Party (CCP) officials and cadres are also common.

Within China's policy research community, military-related think tanks have always constituted a field of their own, or, to be more precise, a "special niche" within the complex and multi-layered context of China's decision-making system. The air of mystery surrounding think tanks and research organizations working in this field is due to two main reasons: on the one hand, the scarcity of publicly accessible primary sources related to the working mechanisms of the military apparatus within the decision-making processes limits outside observers' ability to understand their role. On the other, the sensitivity of the majority of topics discussed on a daily basis by military-related research institutes—from arms control to nonproliferation, from national security to cyber-security—prevent, to a certain extent, Chinese scholars and policy analysts at these think tanks from engaging in open discussions with all but the most well-connected outside observers about their work, further hindering the West's ability to understand military think tanks. **[1]**

However, two trends should be noted when analyzing the current status of military think tanks in China. The first aspect concerns the "human capital" recruited by these organizations. The experts attending meetings and conducting research are often addressed in the West as PLA "officials" or "officers" and many of them are assumed to have served in the military. The reality, however, is that

the vast majority are academics who work for the military, and their "military rank" does not necessarily mean they have served on active duty. Zhu Chenghu (Major General), Pang Zhenqian (Major General) and Xu Weidi (Senior Colonel) are only a few of the numerous Chinese experts attending international conferences on behalf of the Chinese military, and yet, they have never served in the military. Apart from conferences and meetings, they also appear in the Chinese media to speak on TV and write commentaries addressing military affairs, often on U.S.-China military relations. Similarly, they often make harsh criticisms of U.S. foreign and military policy toward China. Their major complaints range from U.S. military exercises close to China's waters to discussion about economic relations with international partners other than the United States, because "these are all measures taken by the United States in order to contain China" (People's Daily Online, January 6). However, there is considerable debate in Western analytical circles over whether they represent an authoritative voice of the PLA (see *China Brief*, July 23, 2013).

Despite this public criticism of the United States, there has been a slow but steady willingness to establish cooperative exchanges with U.S. think tanks. Indeed, in recent years, many Chinese military-related and foreign policy research organizations developed close relationship with U.S. think tanks and research institutions working on security studies through conferences, informal meetings and symposiums. An example is the "Track 2 Sino-US Cyber-security Dialogue" (CSIS, 2009). Inaugurated in 2009, the annual meeting brings together CICIR (China Institutes for Contemporary International Relations), the think tank under China's version of the Central Intelligence Agency, and CSIS (Center for Strategic and International Studies). The dialogue serves as a strategic platform to enhance cooperation and mutual understanding related to cyber-security, a top priority in the U.S.-China relationship. **[2]**

Building Military Think Tanks With Chinese Characteristics

President Xi's proposal for building think tanks with "Chinese characteristics" positions military-related think tanks to enter a "golden era" (*huangjin shiqi*) as titled by *Modern Military* (March 19). As with other research organizations in China, many of these institutes were initially created in the mold of the Soviet Union at the beginning of the 1950s, and therefore, their policy and research production has been, over time, mostly driven by top-down directives embedded in Marxist-Leninist ideology. **[3]** Within the defense and security field, the turning point is considered to be the Third Plenary Meeting of the 18th Congress in 2013, when for the first time top leaders started to seriously consider how to strengthen the Chinese think tank sector. Government plans released in 2014 require all think tanks, including military ones, to develop a clear position on how they will adopt "Chinese characteristics" by 2020, including not only a strong reputation at the international level, but also strict adherence to the correct political orientation (Xinhua, January, 21).

Indeed, from the PLA's point of view, think tanks are an essential resource when it comes to the military's decision-making system. In 2014, an article published in the *PLA Daily* explained the significance of "Chinese characteristics" with regards to military think tanks: "(1) to adhere to the Party's absolute leadership over the army, improving socialism with Chinese characteristics in the military regime in order to achieve the dream of a strong army; (2) to persevere strategic thinking and research implementation in the era of globalization; (3) to insist on the definition of the military apparatus, implementing research with regards to military activity (*xìng jūn yán zhàn*), reinforcing the strategic decision-making system at the level of the Central Military Commission with a focus on national defense, as well as theoretical and practical issues related to secret military operations" (*PLA Daily*, April 2, 2014; *PLA Daily*, April 3, 2014). According to the article in the CDSTIC's journal, *Modern Military*, many institutes, prime among them the National Defense University, have already planned to adhere to President Xi's proposal within the next three to five years, and the main focus will be on the implementation of teaching and research (*Modern Military*, March 19). According to Quan Heng, Deputy Director of the Institute of Economic Research at the Shanghai Academy of Social Sciences (SASS), the plan for the construction of China's advisory bodies would safeguard national and economic security, improves the national administration system and its modernization, push forward innovation-driven and development policies and, more generally, strengthen China's national image and soft power (*PLA Daily*, June 9, 2014).

Moving Toward a "Revolving Door" For the PLA and Others?

The United States, and to some extent Western Europe, has a unique "revolving door" phenomenon in its think tank community of policy elites moving between serving in the government and being at a think tank—under one president, someone may be making policy as a senior official, and under the next administration, they may be advising the government on policy from the outside looking in. Retired Chinese officials increasingly transition into advisory roles at Chinese think tanks, including in the military sector, but few leave government mid-career for the think tank world only to return to government service later. One rare example of a senior think tank scholar going to work for the government is Dr. Qu Xing's appointment to be China's next ambassador to Belgium in December 2014 (Ministry of Foreign Affairs, 2014). He was previously the President of the China Institute of International Studies, the Ministry of Foreign Affairs' (MFA) main think tank, from 2010 to 2014. While this high-level appointment sets a precedent, Chinese scholars have expressed skepticism this would begin to normalize the "revolving door" in China (The Diplomat, January 8).

There are, however, many examples of retired Chinese senior officials "cross-pollinating" between the PLA and government—they are now working in think tanks in a different field from their careers. The China Association for International Friendly Contact (CAIFC), a public front organization for the PLA's foreign outreach, is run by Li Zhaoxing. Li was the Minister of Foreign Affairs from 2003 to 2007 and has been the chairman of the CAIFC since 2008. On the other side, the MFA's CISS staff includes Colonel Teng Jianqun (CISS, 2015). Colonel Teng was previously a PLA Navy officer from 1979 to 1992, and later a research fellow at the PLA's AMS think tank. This "cross-pollinating" may be the closest the Chinese policy community comes to replicating the United States' "revolving door."

Conclusion

Two important dynamics are at play for Chinese military think tanks as they develop under President Xi. First, the increase of "cross-pollination," and potentially the "revolving door," will improve their research focus through enhanced government experience and understanding of officials' analytical needs, and will improve these think tanks' influence on policy as their personal and institutional connections grow. Second, Xi's call for all Chinese think tanks to advance Chinese soft power will, on the one hand, support more outreach and engagement by Chinese think tanks with foreign organizations, but the focus of Xi's efforts on Party loyalty may decrease the quality of this engagement by further restricting the space for independent thinking by PLA academics abroad.

Whether military think tanks will play a bigger role in the Xi administration's foreign policy decision-making, or if the administration will have growing influence and control over military think tanks, remains an open question. President Xi's emphasis on strict adherence to the Party's political directives and efforts to stifle dissent, inside and outside of government, suggest military think tanks will ultimately fall in lock-step with the Party and Xi, without injecting objective analysis into China's foreign policy decision-making.

Silvia Menegazzi, Phd, is Post-doc Research Fellow and Teaching Assistant in International Relations at LUISS Guido Carli University in Rome. Her research interests focus on Chinese think tanks, Chinese foreign policy and China-EU relations.

Notes

1. For a limited Western assessment of military think tanks' role in Chinese decision-making, see Cheng Li, *China Leadership Monitor*.

2. See Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," in *China Leadership Monitor*, October 7, 2013.

3. See Evan Medeiros, "Agents of Influence: Assessing the role of Chinese Foreign Policy Research Organization after the 16th Party Congress," in Andrew Scobell and Larry Wortzel, (eds.), *Civil-Military Change in China Elites, Institutes and Ideas after the 16th Party Congress*, Strategic Studies Institute, 2004, pp. 279–308.

*** *** ***