Pushing Boundaries - Chinese Diplomatic and Military Behavior Intensifies in the Run-up to the 19th Party Congress

Amid rising tensions between the United States and North Korea, Gen. Fang Fenghui (房峰辉) greeted his American counterpart, Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford in Beijing on August 14. Recognizing the necessity of clear communication as the U.S. assesses possible military action against North Korea, the two held talks targeted at "mitigat[ing] the risk of miscalculation in the region" (Takungpao, August 15; Pengpai, August 15).

Although both parties are aligned in their desire for stability on the Korean Peninsula, China's relations with the United States and its neighbors have worsened over the course of 2017. From its border with India, to the East China Sea, China appears to have decided to ratchet up, rather than moderate, areas of friction. In the case of the U.S., tension is rising over possible trade war, right as China is entering an important political season. More than ever, it is important to understand the factors that go into determining China's willingness to use force, expend political capital, and confidence when challenging its neighbors.

A review of China's recent diplomatic and military actions—and their impact on U.S.-China ties—can provide some useful context as both sides attempt to cooperate on North Korea and other issues.

China has achieved a number of important diplomatic successes in the first eight months of 2017. Perhaps the most important progress was seen in China's long attempt to undermine international support for the Republic of China (Taiwan). Particularly after the effective setback the People's Republic of China (PRC) experienced when Democratic Progressive Party candidate Tsai Ing-Wen was elected to the ROC's presidency in 2016, the PRC has made significant headway in reducing the ROC's diplomatic presence abroad.

In January, Nigeria closed a Republic of China trade mission in its capital, Abuja. This followed São Tomé and Príncipe's switch in recognition to the PRC in December 2016 (ROC-Taiwan.org, December 21, 2016). In early June, Panama cut ties with the ROC and recognized the PRC. Taiwan is consistently rated at the top of China's diplomatic and military objectives, and as of August 2017, only 20 nations worldwide recognize the Republic of China. These successes can be expected to embolden China's use of economic diplomacy to effectively sway other countries to support its causes.

In Southeast Asia, targeted Chinese diplomacy and distrust of U.S. commitment to involvement in the South China Sea appears to be having an effect. Little more than a year after an international tribunal ruled in favor of the Philippines' territorial claims in the South China Sea, China enjoys unprecedented influence in Manila. Philippine President Rodrigo Duterte, who regularly criticizes the U.S., has moderated his stance somewhat as he enlists U.S. military support to deal with a terrorist crisis in the south of his country. However, his eagerness to improve ties with China, and plans for large Chinese investments, will remain important parts of his political platform.

To the west, Vietnam has entered a particularly tense stage of relations with China. In July, Vietnam withdrew oil drilling ships in the East China Sea after China threatened military action. This followed earlier tensions in June that resulted in Central Military Commission Vice-Chairman Fan Changlong (范长龙) cutting short his visit (Xinhua, June 18). In both cases the level of animosity, as the two nations maintain close ties at the Party-to-Party level, and have a number of off-ramps to decrease tensions. But with the withdrawal of the drilling ships it is clear who has the upper hand. China's position in the South China Sea—via carrot and stick—is more secure than ever and the lack of major cohesive pushback from Southeast Asian nations is having is generating national confidence in China's rise.

This confidence in dealing with its neighbors is reflected with a generally upbeat feeling among Chinese nationalists at home. On July 1, the PRC celebrated the 20th anniversary of the handover of Hong Kong. The celebrations were meant to emphasize that whatever "One Country, Two Systems" may imply, Hong Kong was firmly part of the Mainland. China's sole active aircraft carrier, the *Liaoning*, visited Hong Kong harbor and hosted current and former Hong Kong Chief Executives—Beijing's appointed stewards—Carrie Lam, Leung Chun-ying and Tung Chee-hwa (SCMP, July 7). Foreign Ministry spokesperson Lu Kang even took a victory lap, stating that the Sino-British Joint Declaration, which had guaranteed a "high degree of autonomy, except in

foreign and defense affairs" through 2047 "no longer has any practical significance nor any binding force on the central government's administration of Hong Kong SAR" (Xinhua, June 30). **[1]** This is understood to undermine the "One Country, Two Systems" plan outlined from Hong Kong, and for PRC-proposed plans for peaceful integration of Taiwan.

In a year that marks the 90th founding of the People's Liberation Army, the Chinese military has made a series of symbolic and concrete advances. Nationalistic, feel-good events included the April launch of China's first domestically produced aircraft carrier. For the PLA, an August celebratory parade—traditionally held in Beijing—was instead broadcast from the Zhurihe training ground and included more realistic operations (see the full analysis of the parade in this issue).

China's diplomatic and symbolic achievements are mirrored, perhaps, in its military's new confidence. Indeed, China's military had a number of real confrontations with its neighbors and the U.S. military.

The Chinese military is also stepping up its long-range patrols near Japan and Taiwan. While the Chinese Air Force frequently visits the 'center-line' between the PRC and ROC (an ROC white paper recorded an average of 1,385 flights per year between 2004 and 2007), they now regularly circle the island and collect electronic information. ROC Ministry of Defense Spokesperson Major General Chen Chung-chi emphasized that these are normal activities (UDN [Taiwan], August 10). **[2]** However, in aggregate the PLA Air Force appears to be increasing its activity. The Japanese Air Self Defense Force continued to see a yearly increase in the number of scrambles to intercept Chinese aircraft. **[3]** In May, a Chinese fighter jet flew upside-down over a U.S.

plane collecting data about North Korean nuclear tests. In a series of incidents during June and July, Chinese jets performed aggressive interceptions of U.S. electronic surveillance aircraft of the East China Sea. While Chinese interceptions of U.S. flights are routine, the decision to allow such unsafe behavior is instructive. And whereas Chinese jets conducting long-distance flights near Japan tend to be lightly armed, if at all, footage of Chinese intercepts reveal they carry a full weapons load when intercepting U.S. aircraft.

Chinese navy ships are traveling much further afield than they traditionally did. A small group from the South Sea Fleet recently participated with their Russian counterparts in the Baltic Sea. Chinese signals intelligence ships were spotted off the coast of Alaska for the first time, likely to observe a U.S. missile test (Sina, July 14).

In mid-June of this year Indian soldiers confronted Chinese troops building a road along the border between China and Bhutan. Although both sides regularly interact at the small unit level at a number of places along the border, in this case the situation escalated. The area is viewed by India and China as a strategic bottleneck, necessary for power, economic and cultural projection in the region (*China Brief*, April 20). In mid-August similar confrontations took place along the western portion of China and India's border near Pangong lake (*Times of India*, August 16). Together, these have pushed Sino-Indian relations to the tensest point since the 1980s.

Political and military decisions are not made in a vacuum. Some military training exercises are routine; sometimes errant behavior escalates

unnecessarily. But overall, policy, and the decision to exert diplomatic or political pressures are the result of deliberate decisions.

Though, not a popular democracy, China's political system still rewards political deliverables—economic growth or other noteworthy achievements play a role in getting ahead for government cadres. The same goes for diplomatic and military achievements. Ahead of the 19th National Congress of the Chinese Communist Party planned for October, there may be increased willingness to more directly challenge the U.S. and its allies.

A second factor to consider is prestige as a motivation for diplomatic and military action. China's successes in both fields have had real effects in increasing Chinese citizens sense of national confidence and pride. Although continuing internal challenges (rising local government and SOE debt, environmental issues and social inequality) and the militaries' shortcomings (lack of realism in training, incomplete reforms) could act as a check on adventurism, more confident military and foreign policy behavior should be expected.

Throughout, the Chinese leadership appears to wish to maintain escalation control: adopting heavy-handed tactics while forcing other countries to acknowledge China's ability to go further if needed.

Peter Wood is the Editor of China Brief. You can follow him on Twitter @PeterWood_PDW

Notes

1. Constitutional and Mainland Affairs Bureau, *Joint Declaration, June 30, 1985* http://www.cmab.gov.hk/en/issues/jd2.htm

2. Republic of China Ministry of Defense, *National Defense Report 2008 p. 85*

3. In fiscal year 2016 the JASDF scrambled fighter jets 871 times compared to 571 in 2015. Ministry of Defense Joint Staff, *Statistics On Scrambles Through Fiscal Year 2016*, *http://www.mod.go.jp/js/Press/press2017/press_pdf/p20170413_02.pdf*

***

The PLA at 90: On the Road to Becoming a World-Class Military?

By Dennis J. Blasko, Elsa B. Kania and Stephen Armitage

China recently celebrated the 90th anniversary of the founding of the People's Liberation Army (PLA) with a parade and military exercises at the Zhurihe Training Base in Inner Mongolia (CCTV, July 30). Although the display was characterized as a demonstration of China's growing military might—particularly new equipment and weapons platforms, including advanced missiles and aircraft—the event also provided important indications of the PLA's approach to operations and the first-ever demonstration of an actual military operation during a parade. The PLA's anniversary celebration thus reflected its progress toward becoming a "world-class military" and confidence despite remaining challenges related to the ongoing, historic reforms. Shortly after the parade, Xi Jinping announced: "The PLA has basically completed mechanization and is moving rapidly toward 'strong' informationized armed forces," achieving the 2020 goal of its

"three-step development strategy" (*PLA Daily*, August 2).

PLA Parades in Perspective

Traditionally, PLA parades such as those held in Beijing in 2009 and the 2015 Victory Day Parade—have tended to be highly choreographed displays that are counterproductive in terms of the force's operational capabilities in actual combat (实战), taking considerable time away from training for the units involved (China Brief, September 24, 2009). For prior parades in Beijing, units from all over the country were required to send personnel and equipment to prepare for the drive down Chang'an Jie months in advance, losing the opportunity to train in a more realistic way for almost an entire training season.

The ongoing military reforms, announced in 2015 and set to continue until 2020, are intended to bridge the gap between the "two incompatibles," the "two inabilities," and "five incapables" relative to where the State and Party need the PLA to be (*China Brief*, May 9, 2013). In other words, the true test for the PLA is whether the units that operate its equipment can actually perform the missions assigned, and that depends on the level and realism of training the units receive and the quality of their personnel. That this parade was organized at a training base at least enabled some units to engage in training while preparing for the parade, reflecting a greater commitment to preparation for combat operations. Additionally, PLA parades have been opportunities to display a vast array of new equipment, which has greater potential capabilities than the older equipment replaced, signaling the military's modernization.

Integrated Combat Operations

The parade itself was centered around the display of the PLA's joint force units responsible for actual operations, known as "operations groups" (作战群) and other support groups (Xinhua, July 31, 2017). In modern combat, the PLA seeks to integrate the capabilities of these various groups in joint "systems of systems operations" (体系作战). Each group was composed of a series of "formations" (*fangdui*, 方队) or aerial formations/echelon (*tidui*, 梯队), which were comprised of units from one or more service or the People's Armed Police (PAP). **[1]** Unfortunately, the parade did not provide new insights about the PLA's evolving organizational structure, which is increasingly centered on combined arms brigades (*hechenglu*, 合成旅). Nonetheless, the formations associated with each operations group revealed the types of weapons and equipment that will be employed in future joint campaigns. **[2]**

In addition to the units that passed in review in the air or on the ground, Xi Jinping also reviewed seven large formations of roughly 900 dismounted personnel each. Across from the VIP reviewing stand, the Central Theater Army's 112th Mechanized Infantry Division set up a static display of tanks, infantry fighting vehicles, and artillery, along with other weapons from the Rocket Force, like the CJ-10 cruise missile. After the ground and air formations had passed, these seven personnel formations ran at "double-time" to form up opposite the reviewing stand,

Operations Group	Formation Name	Source Force/Unit	Equipment
Ground Operations Group (陆上作战群)	Air Assault Echelon/Tidui (空中突击梯队)	83rd Group Army Army Aviation Brigade, reinforced by elements of two other Army Aviation brigades	Z-10 and Z-19 attack helicopters, Z-8B transport helicopters
	Tank Formation (坦克方队)	Army	Type-99A main battle tanks
	Combat Vehicle Formation (步战车方队)	Army	Type-04A and Type-08/09* Infantry Combat Vehicles [3]
	Self-Propelled Artillery Formation (自行火炮方队)	Army	122 mm and 155 self-propelled artillery, PHL-03 300 mm rocket launchers
	Anti-Tank Missile Formation (反坦克导弹方队)	Army	HJ-10 anti-tank missile
Information Operations Group (信息作战群)	Information Support Formation (信息支援方队)	Strategic Support Force	
	Electronic Reconnaissance Formation (电子侦察方队)		
	Electronic Countermeasures Formation (电子对抗方队)	Central Theater Command Army Air Defense Brigade and 112th Mechanized Infantry Division's Electronic Countermeasures fendui (分队)	
	Unmanned Aerial Vehicles (UAV) Formation (无人机方队)	Army and Air Force units	Communication and radar jamming UAVs (likely ASN-209); ASN-301 Anti-Radiation Missiles (ARM)
Special Operations Group (特种作战群)	Special Forces Formation (特种兵方队)	Tibet Military District Special Operations Brigade, "Plateau Snow Leopards" (高原雪豹)	248 commandos in 8X8 all-terrain vehicles
	Special Operations Equipment Formation (特战装备方队)	82nd Group Army Combined Arms Brigade	Light assault and reconnaissance vehicles
Air Defense and Anti-Missile Operations Group (防空反导作战群)	Early Warning Radar Formation (预警雷达方队)	Air Force	
	Air Defense Artillery-Missile System Formation (弹炮系统方队)	Army Division Air Defense Regiment; Central Theater Command Air Force Surface-to-Air Missiles (SAM) Brigade	Type-09 self-propelled anti-aircraft guns, HQ-6 missile launchers, target-tracking anti-aircraft guns
	SAM Formation (地空导弹方队)	Air Force SAM Unit	HQ-9B, HQ-22 SAM systems
Maritime Operations Group (海上作战群)	First Formation of Naval Missiles (海军导弹第1方队)	Navy	HHQ-98 ship-to-air missile, YJ-12A ship-to-ship missile
	Second Formation of Navy Missiles (海军导弹第2方队)	Navy	YJ-83K air-to-ship missile, YJ-62A shore-to-ship missile
	Marine Formation (海军陆战队方队)	Navy	Personnel in Mengshi vehicles
Air Operations Group (空中作战群)	Fighter Jet Echelon/Tidui (歼击机梯队)	Air Force	J-11B, J-16, and J-20 fighters
	Early Warning and Command Aircraft Echelon/Tidui (预警指挥机梯队)	Air Force	KJ-2000 and KJ-500 early warning aircraft, Y-8 command and communications aircraft, Y-8 jammer, J-10B fighters
	Transport Aircraft Echelon/Tidui (运输机梯队)	Air Force	Y-20, Y-9 transport aircraft
	Bomber Formation (轰炸机梯队)	Air Force Division	HJ-6K strategic bombers
	Aerial Refueling Echelon/Tidui (加受油机梯队)	Air Force	HY-6 refueler, J-10C fighter
	Carrier-Based Aircraft Echelon/Tidui (舰载机梯队)	Navy	J-15 fighters
	Airborne Troops (空降兵方队)	Air Force	Airborne Combat Vehicles and Airborne Assault Vehicles
Comprehensive Support Group (综合保障群)	Information and Communications Support Formation (信息通信保障方队)	76th Group Army Service Support Brigade (勤支援旅)	Tropo-scatter and satellite communication vehicles
	Engineering and Anti-Chemical Support Formation (工程防化保障方队)	71st Group Army Combined Arms Brigade Element (合成旅抽组) [4]	Minesweepers, armored engineering vehicles, tactical bridging, decontamination trucks
	Logistics Support Formation (后勤保障方队)	Wuhan Joint Logistics Support Base, Zhengzhou Joint Logistics Support Center	Field ambulances, water trucks, food processing trucks
	Equipment Support Formation (装备保障方队)	83rd Group Army Combined Arms Brigade, Central Theater Command Army Mechanized Infantry Regiment Element	Armored vehicle repair vehicles, armored recovery vehicles
Counterterrorism and Stability Protection Group (反恐维稳群)	PAP Special Police Formation (武警特警方队)	PAP Falcons Commando Unit (武警猎鹰突击队)	168 PAP Special Operations and counterterrorism personnel
Strategic Strike Group (战略打击群)	Rocket Force Formation (火箭军部队方队)	Rocket Force	360 officers and enlisted personnel
	Nuclear-Conventional Combined Missile Formation (核常兼备导弹方队)	Rocket Force	DF-26 IRBM
	First Formation of Conventional Missiles（常规导弹第1方队）	Rocket Force	DF-21D ASBM
	Second Formation of Conventional Missiles (常规导弹第2方队)	Rocket Force	DF-16G MRBM
	Nuclear Missile Formation (核导弹方队)	Rocket Force	DF-31A, DF-31AG ICBM

where they listened to Xi's speech on the requirements for PLA modernization.

A Historic First for Army Aviation

The parade also marked a historic moment for PLA Army Aviation: the first time the PLA has ever executed tactical procedures during a parade, marking the "public debut" of an Army airborne assault unit (China Daily, July 31). The demonstration was conducted by an *air assault brigade* (空中突击旅) from the 83rd Group Army,

supported by elements of two other Army Aviation units (Xinhua, July 30). The air assault simulated the integration of reconnaissance, attack, and transport helicopters with infantry to deliver soldiers to a distant location on a battlefield. It is unclear if the infantry troops transported by the helicopters are assigned permanently to the army aviation brigade.

The air-assault demonstration brought together a series of army-aviation unit maneuvers meant

to display the ability to assault and secure a remote landing zone (China Military Online, July 31). The demonstration involved an initial sortie by a "reconnaissance and alert unit," which flew over the landing zone to determine the situation, followed by a "firepower assault unit" composed of attack helicopters that secure the landing zone by targeting and neutralizing nearby known enemy positions. Finally, three "air-landing units" delivered the infantry troops to the battlefield (here on evenly-spaced concrete pads), where they disembarked and would have proceeded to fight. These units were supported by an escort unit to provide extra firepower. Finally, the troops reassembled at their helicopters and stood by for the remainder of the parade. While not a realistic test of capabilities, this was a major step for a PLA parade—an improvement that added actual value compared to marching or flying straight lines simply for show—while reflecting the progress made by Army Aviation. **[5]**

The Information Operations Group on Display

Notably, the parade also showcased the *information operations group*, a joint-force wartime construct that would bring together the various, disparate elements responsible for cyber, electronic, and psychological warfare into an operational command at strategic, campaign, and tactical levels. Prior to reforms, the national-level or strategic information operations group would have drawn units from the General Staff Department (GSD), the General Political Department (GPD), and the General Armament Department (GAD). The newly-established Strategic Support Force (SSF) has knocked down the silos between these units, incorporating them into a cohesive force in peacetime both to facilitate the transition to wartime and to construct a war-fighting

force capable of achieving dominance in these critical domains (*China Brief*, February 6, 2016; *China Brief*, December 21, 2016).

The information operations group formation itself resolves a few remaining questions on the relationship between the SSF and China's wartime structure for information operations. First and foremost, the parade formally indicates the SSF's role as the primary fighting force for information operations and "information support" (信息支援), which involves C4ISR support in critical, emerging domains like space, cyber, and the electromagnetic spectrum. Like the relationship between the other services and their corresponding operations groups—the PLA Navy with the maritime operations groups, the PLA Air Force with the air operations group, and the PLA Rocket Force with the strategic strike group—the SSF serves as the central component of the information operations group. Secondly, while the SSF is the primary fighting force for information operations, it is not the only one. The SSF only incorporates strategic-level and former GSD, GPD, and GAD units, not those from the theater or campaign-level, which are now part of the new Theater Commands (战区). For instance, the electronic countermeasures (ECM) formation came from the PLA Army, specifically from an air defense brigade and a division's ECM *fendui* (电子对抗分队) (Xinhua, July 30). What is still unclear are the composition of information operations groups of different echelons, whether tactical or campaign-level groups could have a national mission, and how their respective missions would be coordinated or deconflicted.

China's Strategic Deterrence on Parade

The *strategic strike group* showcased the newly-elevated PLA Rocket Force (PLARF), which is

considered the "core force" for China's strategic deterrence (Xinhua, July 30). The PLA's 90th anniversary served as an occasion to display and unveil some of the PLA's most advanced missiles. **[6]** The DF-26, an intermediate-range ballistic missile with a maximum range of 4,000 kilometers, was highlighted as having combined nuclear and conventional (核常兼备) capabilities (Xinhua, July 30). The DF-21D medium-range anti-ship ballistic missile, which has a range of 1,750–2,000 kilometers, would have particular utility against maritime targets and thus is popularly known as the "carrier-killer" missile (Xinhua, July 30). Of its conventional missiles, the PLA also displayed the modified DF-16, a medium-range ballistic missile with a range of 800–1,000 kilometers (Xinhua, July 30).

The parade concluded with the first parade appearance of the DF-31AG, a modified version of the road-mobile DF-31A intercontinental ballistic missile (Xinhua, July 30). The new version could have a range over 11,000 kilometers and greater survivability due to the use of a transporter erector launcher (TEL) that can go off-road, over rougher terrain to enhance its mobility (IHS, August 8). A week before the parade, a model of the DF-31AG was displayed at the PLA Military Museum in Beijing (South China Morning Post, July 24). These dual-capable, conventional, and nuclear missiles constitute integral elements of China's deterrence capabilities that enable regional defense and long-range precision strike. **[7]**

Real Training Off the Parade Ground

Because the parade was held at Zhurihe in the middle of the large unit training season, several units took the opportunity to conduct training that is much more realistic than what occurred on the parade ground. Prior to the parade, elements of the 112th Mechanized Division and the same Army Aviation units that were seen in the parade conducted live fire field training, simulating an actual air assault coordinated with ground maneuvers (CCTV, August 1). Moreover, the parade was preceded by a combined ballistic and cruise missile exercise against mock targets that reportedly resembled U.S. THAAD missile batteries and models of U.S. F-22 stealth fighters (*Fox News*, August 2). This exercise was conducted by units from the Air Force and Rocket Force, which fired live HQ-6, HQ-16, and HQ-22 SAMs and DF-26, DF-16, and CJ-10 ballistic and cruise missiles, respectively (*The Diplomat*, August 3).

Conclusion

Although much of the media coverage to date has focused on the symbolic and political importance of the parade as a powerful reaffirmation of the military's loyalty to the CCP and Chairman Xi Jinping ahead of the pivotal 19th Party Congress later this year, the parade reveals a force that is still growing and developing, concurrently envisioning itself as a modern, advanced military and acknowledging its own weaknesses. The parade demonstrated an important development in the PLA's pursuit of developing improved joint operations capabilities by incorporating the key components necessary for combat operations, supported by information support, electronic warfare, logistics support, and other non-combat units. The air-assault demonstration, the integration of the SSF through the information operations group, and the prominent display of the PLA's latest and most advanced missiles are clear signs of the PLA's developing operational capabilities and evolving force structure. The demeanor of the both PLA leadership and troops indicated a

highly disciplined force. The parade and media coverage both signify that the Party will always command the gun and should not be discounted as a powerful deterrent signal to foreign observers of the PLA's progress and the scope of its ambition.

Dennis J. Blasko, Lieutenant Colonel, U.S. Army (Retired), is a former U.S. army attaché to Beijing and Hong Kong and author of The Chinese Army Today (Routledge, 2012).

Elsa Kania is an analyst focused on the PLA's strategic thinking on and advances in emerging technologies. Her professional experience has included working at the Department of Defense, the Long Term Strategy Group, FireEye, Inc., Harvard's Belfer Center, and the Carnegie-Tsinghua Center for Global Policy. She is fluent in Mandarin Chinese.

Stephen Armitage is a former DOD analyst, US expat and researcher primarily focused on Chinese information operations and emerging tech.

Notes:

1. The terms *fangdui* and *tidui* are used almost exclusively for parades and are not operationally significant.
2. For a full listing of formations in the parade see: PLA Daily, August 1 and related official media coverage.
3. The coverage of the parade refers to the Type-08 infantry fighting vehicle. However, previously that eight-wheeled vehicle was called the Type-09, ZBD09, or ZBL-09.

4. The term 抽组 (chouzu) is typically used to refer to a group, element, or detachment selected from a larger unit.
5. In the early 1990s, the PLA Army only had about 100 helicopters, none of which were attack helicopters. At present, the PLA Army has over 1,000 helicopters in at least 14 operational brigades in all group armies and the Xinjiang Military District, and is half the size of the PLA Army in the early 1990s (NetEase). For comparison, the U.S. Army, at 465,000 personnel, less than half the size of the PLA Army, has roughly 4,000 helicopters and has been conducting air assault operations in combat since the mid-1960s (DOD, May 31). See: The Military Balance 2017, International Institute for Strategic Studies, London, pp. 46, 48.
6. Please note that all details on missile ranges are taken from the Department of Defense's Report, "Military and Security Developments Involving the People's Republic of China 2017," https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770.
7. Note that although the DF-31 was included in the 1999 parade, it was not until 2006 that the U.S. Department of Defense declared it had achieved "initial threat availability." (See: DoD Report to Congress 2007, p. I.) The status of the DF-31AG has not been confirmed at this point.

Counterintelligence Remains Weakness in Taiwan's Defense

By Peter Mattis

On July 6, Taiwanese authorities charged recently-graduated Chinese student Zhou Hongxu with espionage, roughly four months after he was first detained on suspicion of spying for Beijing (Central News Agency [Taiwan], July 6). The young man, who attended National Cheng-chi University, allegedly attempted to pay a junior Foreign Ministry official with cash and travel for classified government papers (*Taipei Times*, March 11). In 2009 then-President Ma Ying-jeou opened the flow of people and business across the strait without consulting security officials on how to mitigate the risks. Zhou's case is one of the first public espionage cases of Beijing exploiting the ability to send intelligence operatives directly to the island enabled by that law. Zhou's arrest highlights the challenges President Tsai Ing-wen faces—not only from increasingly aggressive Chinese intelligence and influence operations—but also in developing more effective countermeasures absent a clear consensus of the China threat inside and outside her party.

Despite Beijing's relentless and sometimes fruitful efforts to penetrate the most sensitive parts of Taiwan's national security institutions and society, Taiwan's leaders have not been able to push forward a stronger legal foundation for counterintelligence. In March, Tsai's cabinet vetoed new security regulations over legitimate concerns about overreach, and the failure of the Legislative Yuan to push forward new legislation leave Taiwan vulnerable. Without such tools, the island's counterintelligence professionals can observe the change in scope and intensity of China's operations but are unable to act effectively. The problem is worsened because the Kuomintang (KMT) and the Democratic Progressive Party (DPP) struggle to find common ground despite their shared interest in not allowing Beijing to decide Taiwan's future.

Chinese Intelligence Presses Onward

In addition to Zhou, two other major Chinese espionage cases struck Taiwan in earlier this year that penetrated the most sensitive areas of national security. The first is Wang Hung-ju, Vice President Annette Lu's former bodyguard, who was arrested because of his connections to an espionage case cracked in 2010 (Taiwan News, March 16). The second is the former commander of the Air Defense Command, Hsieh Chia-kang, who may have begun spying as early as 2009 or 2010 (*China Post*, May 12).

The Wang Hung-ju case probably is the more important of the two cases, because of his connections to Taiwan's intelligence agencies and leadership protection details. Wang was a former official in the Special Service Command Center in the National Security Bureau. Mr. Wang served for a short period as the bodyguard for Vice President Annette Lu before retiring in 2003 (*Taipei Times*, March 17). After his retirement, he traveled to China where he was recruited by the Tianjin State Security Bureau in 2009. **[1]** Wang attempted to recruit two friends into his intelligence network, including an officer in the Military Police Command (*United Daily News*, May 12). The links between Wang's case and Taiwanese businessman Ho Chih-chiang's are unclear, but Taiwanese press repeatedly reported that Wang was uncovered as part of the Ho investigation. Chinese intelligence, possibly the Tianjin State Security Bureau, recruited Ho in

2007 and used him to approach Taiwanese intelligence officials. Ho's case officers empowered him to offer money and other inducements to recruit serving officials (Focus Taiwan, April 15, 2010). Such intermediaries are typical of Taiwan's espionage cases, especially when they involve the military, and their discovery may lead to multiple Chinese spies as the authorities work back on a case (China Brief, November 7, 2014).

In May, Taiwanese authorities detained a serving major general, Hsieh Chia-kang, and a retired colonel, Hsin Peng-sheng, for selling secrets to China. At the time, Hsieh was serving as the deputy commander of the Matsu Defense Command and had overseen the Air Defense Command. In the latter position, he would have had access to the specifications for the U.S.-made Patriot missiles as well as the Taiwanese Tien-kung III and Hsiung-feng 2E cruise missiles. Chinese intelligence recruited Hsin while he was leading a Taiwanese tour group in China. Hsin allegedly recruited Hsieh with whom he had served years before. According to the prosecutors, Hsieh traveled to Malaysia and Thailand to meet his handlers, and his travel suggests he may have been working for Chinese intelligence since 2009 or 2010. Both men agreed to assist Chinese intelligence in identifying and recruiting other sources (Liberty Times, May 10; Taipei Times, May 11; China Post, May 12).

While these two cases represent traditional methods of Chinese intelligence, Zhou Hongxu's case is different in that he is part of the large group of mainlanders able to visit Taiwan after 2009. Zhou originally came to Taiwan in 2009 as an exchange student from Zhejiang University and returned to the island in 2012 for graduate studies in business administration at National Cheng-chi University (NCCU), where he earned a

degree in 2016. He returned to China after completing his degree in July 2016 but came back to Taiwan in February on a business visa to work for Taiwanese firm. In addition to attempting to ply a Taiwanese diplomat with cash and an all-expense paid trip to Japan, prosecutors alleged Zhou attempted to conduct intelligence work while an NCCU student, and he built a network of contacts that may have touched senior Kuomintang figures (Taipei Times, March 11; United Daily News, March 11). Zhou's exact role remains out of the public view. His attempted recruitment of a MOFA official suggests that he is an intelligence officer. However, many Chinese intelligence operations involve a case officer inside China and a principal agent outside China, like Ho Chih-chiang or Hsin, recruiting and handling sources (China Brief, November 7, 2014).

Such operations also are well-known to U.S. counterintelligence and would not be unusual. A recent criminal affidavit related to the arrest of State Department secretary Candace Claiborne noted that Chinese intelligence employed "cut-out" or "co-optees." According to the FBI, these are:

> mutually trusted person[s] or mechanism[s] used to create a compartment between members of an operation to enable them to pass material and/or messages securely. A cut-out or co-optee can operate under a variety of covers, posing as diplomats, journalists, academics, or business people both at home and abroad. These individuals are tasked with spotting, assessing, targeting, collecting, and running sources (U.S. Department of Justice, March 29).

Using cut-outs and co-optees may have been the typical Chinese approach, Taiwanese reporting on China's intelligence operations suggests change may be in the air. If Zhou was an intelligence officer, then the case suggests Chinese intelligence is moving toward a more proactive approach to collection rather than just exploiting Taiwanese who come to China. Meetings in Southeast Asia, including Singapore, are apparently more common, and the Zhou case shows Japan is also considered an acceptable third-country meeting site. Using third-country meeting sites can hide the China connection once typical of Taiwan's espionage cases, making it more difficult for Taiwanese counterintelligence (Taiwan News, March 16; *China Brief*, July 1, 2011).

Speaking to Taiwan's Legislative Yuan in March, National Security Bureau director Peng Sheng-chu said "China will employ all methods [of espionage], and the issue [of Chinese infiltration] is more serious than ever" (*Taipei Times*, March 10). It might be easy to read Peng's remarks as a standard warning, but the author's recent discussions in Taiwan indicate that covert Chinese activities have increased in scope, sophistication, and intensity. For the first time in many years, Taiwan's national security officials see change rather than continuity as a hallmark of Beijing's intelligence and subversive operations. What is not clear is whether they have the political support to counter such Chinese operations effectively.

Breakdown on Counterintelligence Bill Leaves Gaps

The most significant proposal put forward to address the Chinese espionage and infiltration threat collapsed amid valid concerns of executive overreach and intrusions on civil liberties.

Although the DPP cabinet vetoed the law before releasing any details, the draft generated controversy because it resurrected policies from the Martial Law Era. The law would have authorized the establishment of security offices at all levels of government, an additional security agency with overlapping authorities with existing organizations, and easier access to suspected spies' private background information (*Taipei Times*, March 17).

According to administration spokesman Alex Huang, the Tsai administration had "already taken measures to evaluate the national intelligence security situation and has established mechanisms to oversee security improvements" (*Taipei Times*, October 2, 2016). Some of those measures are necessarily secret and cannot be confirmed. One of the few public measures enacted by the present administration extended the time for which retired government officials needed to report their foreign travel, especially to China. In early March, the Cabinet revised the regulations governing cross-strait interaction, banning political appointees and senior military officials from traveling to China for three years after retirement (Focus Taiwan, March 3). The Tsai administration has taken two major steps to strengthen Taiwan's organizational capacity for cybersecurity: establishing a department for cybersecurity within the Executive Yuan in August 2016 and creating the Information, Communications, and Electronic Force Command on June 29. Both organizations have far-reaching responsibilities across the government and should provide better information controls as well as the capacity for new secure network infrastructure (Executive Yuan, April 28; Taiwan Today, July 3). Other legislative measures, such as revising the National Security Act to increase the punishment for spying, are still being considered (Focus Taiwan, March 16). The public measures also

hint at internal administrative changes to better handle classified information and improve security reviews of officials holding clearances. Although such changes improve counterintelligence, they do little to address the threat of Beijing's subversion.

The challenge for Taiwan, however, is as much about discretion and awareness as dealing more effectively with China's efforts to penetrate Taiwan's democratic institutions and society. Many retired Taiwanese generals travel to China, attending political events and allowing themselves to be used as political props. Even within KMT circles, such visits have been controversial with former KMT Premier and Taiwan's longest serving Chief of the General Staff Hau Pei-tsun calling for generals to be stripped of their pensions (*South China Morning Post*, August 28, 2015). The most recent uproar over such travel occurred after 32 generals traveled to China to attend an event commemorating Sun Yat-sen presided over by Xi Jinping, but such public appearances have troubled Taiwan for years ([China Post](#), November 18, 2016; [China Brief](#), October 14, 2011). In another case of poor judgment, DPP legislators raised concerns about National Defense University professor Chang Ching has become a regular guest on Chinese military shows while still holding a security clearance without immediate consequence (*Taipei Times*, July 29). Taiwan's premier, Lin Chuan, said it well when he observed that former officials "are high-profile figures in society and their deeds and words must not compromise the national interest" ([Focus Taiwan](#), March 3).

No Consensus on Looming China Threat

Strangely, Taiwan continues to debate the kind of threat Beijing poses and Chinese intentions toward the island. Not everyone shares the clarity exhibited by Mainland Affairs Council Katharine Chang when she told Legislative Yuan members that there are no Chinese hawks or doves in dealing with Taiwan ([Taipei Times](#), March 11). Significant groups within both the DPP and KMT choose to hide behind dangerous illusions of the Chinese intentions toward Taiwan, based in part on recent conversations in Taipei.

Many in the DPP appear to think China's threat to Taiwan can be mitigated by reducing the island's economic dependence on the People's Republic or that preserving Taiwan's international space will be enough. Although such measures as exemplified in Tsai's "Going South" policy may benefit Taiwan, Southeast Asia can never provide the political or economic counterweight to China. DPP leadership also seems willing to allow the party's distrust of the national security apparatus—rightfully developed because of persecution during the KMT's dictatorship—to undermine the interactions between the political and professional staffs. This may be the first time that Taiwan's National Security Bureau has not had a senior official assigned to the National Security Council. A lack of regular contact or trusted intermediaries serves no one well. As Enoch Wu, a Taiwanese think tank scholar, wrote earlier this year, Taiwan's political leadership on both sides has sapped military readiness, under-staffed national security, and lowered morale (*New York Times*, May 18).

The KMT's answer to the Chinese threat runs through Beijing, based on the belief that a stable relationship will protect Taiwan. In March, KMT mouthpieces criticized the DPP for manufacturing the Zhou case to destabilize the cross-strait relationship, move the two sides further apart,

and consolidate a "green terror" with the counterespionage bill (*United Daily News,* March 10; *United Daily News*, March 11; *Taipei Times*, March 17). Little mention was made of the fact that China's intelligence operations never abated during the Ma years. Between 2008 and 2016, Taiwanese authorities publicly uncovered more than 50 cases of espionage and, according to an anonymous official, many more have not been prosecuted (*Taipei Times*, March 11; *Liberty Times*, March 13).

Foreign Pressure and Influence Operations

The absence of strategic clarity and consensus is striking in the face of Chinese activities against the island across a broad front. Beijing continues its campaign to erase the name "Republic of China" from international politics. China continues to entice countries that recognize Taiwan, and Panama switched diplomatic recognition to Beijing in June. Taiwanese arrested overseas in places like Cambodia, Kenya, and Spain have been extradited or deported to China rather than returned to Taiwan (*Liberty Times*, June 14, 2016; *Taipei Times*, August 6, 2016; *China Post*, February 19). Chinese pressure forced Taiwan's representative offices in Nigeria remove "Republic of China" from their name, and Beijing also placed pressure on Dubai and Ecuador (Central News Agency, June 14). None of these things are new, but illustrate that Beijing's pressure has never relented.

Accompanying the rise in espionage operations against the island, Beijing's effort to shape or even destabilize Taiwanese society itself through united front work is intensifying. The aim, according to several Taiwanese interlocutors, is to create a "fake civil society" that can be used against Taiwan's democratic system. Taiwan's national security authorities recently revealed

that China has been active in disseminating disinformation about the Tsai administration's controversial pension reform plans through the popular LINE messaging app and content farm websites (*Liberty Times*, July 18). Beijing also supports China Unification Promotion Party (CUPP) led by former organized crime figure Chang An-Lo, also known as the "White Wolf" (白狼). The CUPP has been one of the significant forces in organizing the pension reform protests and organizing demonstrations when President Tsai travels around Taiwan in an effort to discredit the DPP administration. Chang also has acknowledged cooperating with China's United Front Work Department, which rallies the Chinese Communist Party's friends at home and abroad to exert influence (Taiwan Foundation for Democracy Bulletin, July 18; *China Brief*, July 6; Reuters, November 26, 2014). Concerns about these and other Chinese activities are pervasive across Taiwan's government, but countermeasures are largely being left to the national security agencies themselves within their existing authorities and restrictions.

Conclusion

While Taiwan faces an espionage and subversion challenge from China at a scale that no modern democracy has faced, its leading political parties struggle to address the problem. Despite the stark divide between the DPP and KMT's visions of Taiwan's future, both sides share concerns that China is attempting to force an accommodation on Beijing's rather than Taipei's terms. Yet, neither side seems to trust the other enough to see the need for effective democratic controls over counterintelligence or build a consensus on how to address Chinese subversion. As China helps build a "fake civil society," any Taiwanese government, whether DPP or KMT, will face Chinese pressure from within

and without. The absence of a strong legal framework and a political consensus exacerbates the challenge of counterintelligence and countering covert influence in a democratic society. The stakes are not trivial spy-vs-spy games but the integrity of Taiwan's democracy, and the weakness is every bit as crippling as an ill-equipped or poorly-prepared military.

Note:

1. The Ministry of State Security (MSS) is a sprawling organization centered on a ministerial headquarters in Beijing with provincial departments and municipal or county bureaus. MSS units at every level run domestic intelligence and internal security operations. Several of the larger, more sophisticated provincial-level departments, such as the Guangdong State Security Department, Tianjin State Security Bureau, and the Shanghai State Security Bureau, also conduct foreign intelligence operations against external targets.

Peter Mattis is a Fellow in the China Program at The Jamestown Foundation, where he served as editor China Brief from 2011 to 2013. He is the author of Analyzing the Chinese Military: A Review Essay and Resource Guide on the People's Liberation Army (2015).

***

Disruption Under the Radar: Chinese Advances in Quantum Sensing

Elsa B. Kania and Stephen Armitage

This piece builds upon prior research and analysis on Chinese advances in quantum information science and quantum technologies, previously featured in China Brief in the series "China's Quantum Leap," parts one *and* two*.*

Today, technologies that harness the "spooky" properties of quantum phenomena, once purely science fiction, are fast becoming a reality. Backed by the Chinese leadership at the highest levels, Chinese scientists are achieving rapid progress in a variety of different applications, including quantum encryption—which creates uncrackable communication—and quantum computing, which will enable tremendous computing power that could render most modern forms of encryption obsolete. While each of these technologies could rewrite the rules of how information can be used and processed, quantum sensing—the use of quantum entanglement to enable extremely precise measurement—could most fundamentally alter operational realities of future conflict.

Quantum sensing could be used in a number of technologies with direct military applications. In particular, quantum radar can be used to detect targets that cannot be discerned through conventional radar, and quantum navigation similarly leverages quantum properties to create a precise form of positioning system that may eventually replace GPS. Together, such technologies could be critical to China's future military capabilities and might become a key focus of U.S.-China technological competition.

Context for China's Advances in Quantum Information Science

China has undertaken a massive national campaign to become a world leader in quantum information science. Driven by concerns about potential adversaries' signals intelligence capabilities, the Chinese leadership sees quantum technologies as both a means of security and a strategic enabler to bridge the gap between its military capabilities and those of its potential adversaries. As such, quantum information science programs have been backed by significant state funding across a variety of laboratories and research institutes. Of note, the Chinese Academy of Sciences recently established the Quantum Information and Quantum Science and Technology Innovation Research Institute (中国科学院量子信息与量子科技创新研究院), and China also plans to establish a national quantum information science laboratory (CAC, July 12). Although it is difficult to quantify the full amount of funding that has been devoted to these efforts, anecdotally, Chinese research in this domain is said to receive virtually "unlimited" funding due to its high-level prioritization.

- The new National Key Research and Development Plan (国家重点研发计划) includes basic research on quantum control and quantum information among its prioritized projects (MoST, February 16, 2016). The available guidance (指南) for this project in 2016 and 2017 included quantum precision measurement (量子精密测量) (MoST, August 1, 2016)

- The Thirteenth Five-Year Science and Technology Innovation Plan as a new mega-project highlights quantum navigation (量子导航) (State Council, August 8, 2016) .

- Of note, the PLA's Equipment Development Department is supporting research in quantum technologies through the National Defense Key Laboratories Fund (国防重点实验室基金), which has provided funding for several relevant projects under the Thirteenth Five-Year Plan (Equipment Development Department, May 19).

These programs have started to enable significant advances in quantum communication and quantum computing. In 2016, China launched the world's first quantum satellite, Micius, which could become the first piece of a global quantum network for uncrackable communications (Science Mag, June 2017). In March, Chinese scientists succeeded in entangling 10 superconducting qubits, an important step towards future quantum computing (Physics World, April 2017). In early August, Chinese scientists announced their success in experiments involving Micius, not only demonstrating successful ultra-long-distance quantum teleportation, a key step towards a global "quantum internet," but also succeeding in the first-ever realization of space-to-ground quantum key distribution, a milestone for quantum communication (Nature, August 9, 2017; Nature, August 9, 2017; Xinhua, August 10, 2017). While these developments have received considerable attention in official Chinese and international media, Chinese scientists have also actively pursued advances in quantum sensing, which have often remained below the radar.

Ongoing Research and Development Efforts in Quantum Radar and Navigation

To date, details about China's progress in quantum sensing has been relatively limited, likely because of its more obvious and direct military

applications. Despite these constraints, it is possible to evaluate initial advances in quantum radar and quantum navigation. Of particular note, China's apparent success in the development of quantum radar was prominently featured in September 2016, when Chinese scientists announced their creation of a single-photon quantum radar, which takes advantage of entanglement between photon pairs, capable of detecting targets up to 100 kilometers away with high accuracy (*PLA Daily*, September 13, 2016; CETC, September 18, 2016). Reportedly, the range of this quantum radar was five times that of a laboratory prototype jointly created in 2015 by an international team of researchers (Phys.org, February 26, 2015). This test appeared to constitute a notable advance and an indication that Chinese research in quantum sensing has already progressed considerably.

Despite the limitations of the available information, it is nonetheless feasible to gauge advances to date in quantum radar and quantum navigation based on a review of ongoing research and development efforts in these technological domains. Although this listing is not comprehensive, it provides an initial overview of the scope and scale of these efforts.

Quantum Radar

- The quantum radar prototype reported last fall was developed by the China Electronics Technology Group Corporation (CETC) 14th Research Institute (中国电子科技集团第 14 研究所) Intelligent Sensing Technology Key Laboratory (智能感知技术重点实验室) (CETC 14th Research Institute, September 7, 2016). Earlier papers published by the same group indicates that their research on quantum radar

dates back to at least 2014 (CQVIP, January 2014).

- CETC's 27th Research Institute was also involved in the quantum radar prototype, while CETC's 38th Research Institute has written on and may also be pursuing research on quantum imaging and quantum radar and their development to enable remote sensing (CQVIP, January 2014).

- This quantum radar prototype was developed in collaboration with leading Chinese quantum physicist Pan Jianwei and his colleagues at the University of Science and Technology of China (USTC), which, under Pan's leadership, has become a driving force behind China's quantum advances and hosts the Chinese Academy of Sciences Key Laboratory of Quantum Information.

- The China Aerospace Science and Technology Corporation (CASC) Second Academy has received funding through the National Defense Key Laboratories Fund for a project that examines the characteristics of light scattering and radiation under quantum detection (All-Military Weapons and Equipment Procurement Information Network, June 19)

- The CASC 5th Academy's 508 Research Institute established a Quantum Sensing Laboratory (量子遥感实验室) in 2012 (China Space News, July 26, 2012).

- The CASC 9th Academy's 13th Research Institute has been engaged in research on quantum imaging, which involves the use of quantum correlations for a new

form of remote sensing (CASC, August 20, 2015).

- The Xi'an University of Electronic Science and Technology has received funding through the National Defense Key Laboratories Fund (重点实验室基金) to leverage quantum effects to enhance the performance of radar systems' detection, imaging, and identification capabilities (All-Military Weapons and Equipment Procurement Information Network, June 19).

- The Equipment Development Department is funding two projects each on microwave quantum radar technology and foundational research for quantum radar systems. Each project will receive 500,000 RMB (about $75,000) in funding (All-Military Weapons and Equipment Procurement Information Network, April 11).

Quantum Navigation:

- The Beijing Automation and Equipment Control Research Institute (北京自动化控制设备研究所) reportedly achieved a breakthrough in quantum navigation in a project that pursued key technologies associated with a magnetic resonance spin gyroscope (Xinhua, April 2, 2016). This advance used the quantum property of spin to enable inertial navigation and reportedly established a foundation for future developments in quantum navigation in China.

- The Shanghai Jiaotong University Quantum Sensing and Information Processing Research Center (量子感知与信息处理研究中心), established in 2001, has pursued re-

search on quantum navigation and positioning technology, as well as also quantum sensing and perception technologies (Shanghai Jiaotong University).

- The PLA's Equipment Development Department is funding a project on the exploration of precision guidance systems that leverage new concepts, new principles, and new technologies, including quantum correlation imaging and detection (All-Military Weapons and Equipment Procurement Information Network, August 1, 2016).

The number of research institutes pursuing quantum radar and navigation, as well as the funding available through national science and technology plans, hint at a state-driven national push to advance these technologies. The reports of prototypes and apparent advances also indicate that Chinese researchers may be making real strides toward the operationalization of these quantum capabilities.

Patents Point to Progress

To date, Chinese scientists and research institutes have filed a number of patents related to quantum radar and quantum navigation. Overall, the number of Chinese patent filings in quantum information science tend to rank first in the world or second to the U.S. (*The Economist*). While the ecosystem for research and development described above indicates the scope and scale of these efforts, available patent filings are perhaps a better gauge of real progress:

Quantum Radar

- Since 2010, several scientists have filed quantum radar-related patents, including

researchers affiliated with Zhejiang University, who filed for a patent on laser radar based on strongly correlated quantum imaging (Google Patents, May 7, 2010). In 2012, a researcher filed for a patent of a quantum entanglement radar design (Google Patents, June 15, 2012).

- In 2014, a researcher from the Air Force Early Warning Institute who had previously published several articles on quantum radar filed a patent for quantum radar and target detection methods with intended utility in strategic early warning (Google Patents, October 22, 2014).

Quantum Navigation

- In 2010, researchers from the Xi'an University of Electronics Science and Technology filed a patent for a new method of high-precision navigation and positioning based on quantum properties (Google Patents, July 30, 2010).

- In 2011, researchers with the Chinese Academy of Sciences' Xi'an Optics and Fine Mechanics Research Institute filed a patent for leveraging quantum entanglement to improve the positional accuracy of Beidou (Google Patents, August 25, 2011)

- In 2016, researchers with the PLA Air Force Engineering University filed a patent for a navigation method based on quantum-entangled microwaves (Google Patents, October 28, 2016).

Although it is difficult to evaluate the maturity of this research from the information provided, several of these patents serve as at least a rough

indication that these research efforts have reached a point such that future applications and intellectual property has become a concern.

The Military Applications and Strategic Implications of Quantum Sensing

China's rapid advances in quantum information science and the associated technological applications demonstrate its ambitions to lead global innovation in such strategic frontier (战略前沿) technologies. Relative to quantum computing and quantum encryption, quantum sensing has the most direct and impactful military applications. As the electromagnetic spectrum becomes increasingly crowded in times of peace and contested in times of war, the ability to ensure trust in sensors and operate independently of the spectrum's limitations will be critical. Certain applications of quantum sensing, including quantum radar, imaging, and navigation, could change the dynamic and use of the spectrum in ways that could be highly disruptive in future warfare.

Potentially, quantum radar could nullify stealth technologies and advanced forms of radar jamming. In this regard, the realization of quantum radar could enable the PLA to overcome superior U.S. stealth capabilities, undermining this critical pillar of U.S. military power. Indeed, commentary in PLA media at the time the test of a prototype quantum radar was announced highlighted quantum radar as the "nemesis" of today's stealth fighter planes with "remarkable potential" on the future battlefield (*PLA Daily*, September 22, 2016). In addition, more theoretical descriptions of quantum radar suggest that it could be able to defeat radar jamming techniques, such as digital radio frequency memory (DRFM) jammers, which spoof a radar's broad-

casted signal to conceal an aircraft's true location. Either application would nullify or significant limit the use of both passive (stealth) and active (DRFM jamming) electronic countermeasures in enemy space.

In any potential conflict with China, the use of stealth would be a strategic imperative for the U.S., critical to enable naval vessels to come within striking distance of the Chinese mainland and for aircraft to penetrate Chinese airspace to hold Chinese operational assets at risk. Therefore, quantum radar would be massive disruptive force—an "offset technology"—within the PLA's suite of anti-access/area denial (A2/AD) or "counter-intervention" capabilities. If operationalized, quantum radar could not only undermine the U.S. advantage in stealth but also inherently increase the potential costs of war, forcing the United States to accept higher operational risk and nullifying billions of dollars spent on stealth coating for platforms operating in the Western Pacific.

Looking forward, quantum technology could have major implications for multiple aspects of future military operations. The U.S. Air Force Scientific Advisory Board noted in a recent report that quantum clocks and quantum sensors would merit further investment, since enhanced timing precision could enhance Air Force missions and capabilities, including SIGINT, counter-DRFM, electronic warfare (EW), and also more robust communications (AFSAB, 2016). The same report noted that quantum magnetometers, which enable quantum navigation, could be "an important part of achieving GPS-denied advantage," including because quantum inertial sensing is not susceptible to jamming.

Similar logic about the utility of quantum navigation is evidently at play in PLA thinking. The realization of quantum navigation could allow for a "new generation of inertial navigation," enabling high-precision navigation without GPS, as researchers from the National University of Defense Technology have noted (CNKI). This so-called "quantum compass" would be particularly useful for submarines and other maritime platforms for which it could enable the pinpointing of their position with high levels of accuracy. Quantum navigation could thus potentially liberate Chinese operational platforms from dependence on space-based positioning systems, which can be easily jammed, while the PLA concurrently becomes ever more able to hold U.S. space systems at risk through advancing its counterspace capabilities.

Quantum Uncertainties and Future Developments

Could China surpass the U.S. in quantum sensing? Certainly, active Chinese efforts to pursue advances in quantum radar and navigation, supported and accelerated by the ample funding devoted to quantum information science, demonstrate the PLA's focus on the pursuit of innovation in emerging technologies with highly disruptive applications. Since research and development appear to remain at the prototype stage for the time being, the potential and timeframe for their realization on the battlefield remain uncertain at this point. While technologies like quantum computing and encryption would offer relatively balanced, though disruptive, capabilities, the likely asymmetries in operations for China and the U.S. creates conditions such that quantum sensing, and quantum radar in particular, could give China a much greater advantage at the expense of core aspects of U.S. military power, such as stealth. Considering the disruptive potential of quantum radar and navi-

gation, the PLA's progress in these quantum capabilities reflect an integral aspect of its efforts to compete with the U.S. in technological and defense innovation.

Elsa Kania is an analyst focused on the PLA's strategic thinking on and advances in emerging technologies. Her professional experience has included working at the Department of Defense, the Long Term Strategy Group, FireEye, Inc., Harvard's Belfer Center, and the Carnegie-Tsinghua Center for Global Policy. She is fluent in Mandarin Chinese.

Stephen Armitage is a former DOD analyst, US expat and researcher primarily focused on Chinese information operations and emerging tech.

***

Managing the State: Social Credit, Surveillance and the CCP's Plan for China

By Samantha Hoffman

On July 20, the Chinese government released its *Next Generation Artificial Intelligence Development Plan*. **[1]** The plan has gained significant media attention in part because it links AI with another topic that has drawn a considerable amount of attention, China's "social credit system" (社会信用体系). Social credit uses big-data collection and analysis, to monitor, shape and rate individual's behavior. While advances in artificial intelligence, and the growth of the surveillance state are all noteworthy on their own, China's social credit program explicitly links them as parts of a broader political control process known as "social management" (社会管理).

The phrases "social management", and the more recent version "social governance", may seem like pseudo-scientific jargon, but in fact, are given clear importance by China's top leaders. **[2]** In 2016, General Party Secretary Xi Jinping highlighted the concept, noting: "people working in political and legal affairs and comprehensive social governance have focused on dealing with outstanding problems and innovating *social governance methods* in recent years, achieving greater results," (Xinhua, October 12, 2016). Elsewhere, the Party has clearly explained that it sees operationalizing social management as its blueprint for maintaining power. Far from being a narrow, isolated political concept, "social management" gives cohesion to an array of concepts ranging from Hu Jintao's signature "Scientific Development" to Xi's push for military-civil integration, as part of this power maintenance process (People.com.cn, April 17).

Social Management

Social managements' roots are in the core ideology of the Chinese Communist Party. The CCP defines itself as the "vanguard of the people"—the Leninist idea that a small group of scientifically guided and educated cadres can lead the people in the direction of social equality and prosperity. Mao Zedong's organizational guide, the "mass line" describes the same concept. The CCP leadership is explicitly at the top of this hierarchical mass line system. It takes the "scattered and unsystematic ideas of the masses" and forms them into "concentrated and systematic ideas" before taking them back to the masses to "propagate and explain these ideas until the masses embrace them as their own"—Meaning management along scientific principles. **[3]**

Social management describes a "scientific" Leninist machinery for shaping, managing, and responding. It is best summarized as a complex systems management process through which the Party leadership attempts to manage the Party itself, and through which Party leadership attempts to manage the Party's interactions with society as a whole. Social management is aimed at ensuring China's "holistic" or "comprehensive" state security (国家安全). This holistic state security concept is not fundamentally new under Xi Jinping. It includes the western "national security" concept, but, more significantly, is focused on two internal security dimensions. First, managing the Party itself, and second is managing social order (Xinhua, April 15, 2014; *Qiushi*, April 15, 2017; *PLA Daily* [archive], December 13, 2000).

Social management itself is not a new concept and dates to the PRC's founding in 1949, when it was first integrated into the CCP's discussion of law and social order. The concept became increasingly prominent in the Party leadership's rhetoric between the late 1990s and early 2000s. When the 12th Five-Year Plan for National and Social Development was released in March 2011, social management was enshrined as a key objective (China.com.cn, March 16, 2011). In the plan, the Party set targets for speeding up the construction of a social management system that combined governance measures to address problems at their source, dynamic management, and emergency response—while adhering to the core leadership of the Party.

In its ideal form, the social management process optimizes interactions vertically (within the Party), horizontally (between agencies), and holistically, between the Party and society. At every linkage, the goal is to improve governance capacity to shape, manage, and respond to social demands. Social management must efficiently solve problems to succeed. Such problems include: allocation of public resources, preventing and controlling risks associated with man-made and natural disasters, stopping dissent, and pre-empting and managing social conflict. The process involves both coercive and co-optative tactics, constantly acting together, to force individuals and to incentivize individuals to participate in social management.

For the social management process to succeed, particularly when in a crisis response mode, an automation of the interactions between the state and society, as well as the interactions within the Party itself, is required. The modern-day "grid management" (网格化管理) and the "social credit system" (社会信用体系) are unique compared to previous versions of similar social control mechanisms because they employ modern technology. They represent the attempted automation of social management.

The concept of automating social management is not new under Xi Jinping (2012-Present) or his predecessor Hu Jintao (2002-2012). In fact, the concept emerged in the late 1970s when "social management" was directly connected to complex systems theories the Party-State's theorists were drawing from to design a *Leninist* governance system to recover power after Mao and the Cultural Revolution. The basic ideas originated around 1957 when Qian Xuesen ("father of Chinese rocketry") called on the Chinese Academy of Social Sciences to take the concept seriously as a way of solving social problems [People's Daily [archive], 28 May 1957]. By the 1970s and throughout the 1980s complex systems thinking [largely via Qian Xuesen's promotion of engineering cybernetics] was clearly tied to "social management". For example, one report from 1984, "On the New Technological Revolution"

(新技术革命) said:

> Leaps and bounds in science and technology [since the 1940s have] influenced or given rise to transformations in the way social management agencies work. The theory and practice, perspective and method of systems engineering were born and developed from these changes." It elaborated that it is impossible to manage effectively through individuals or a small number of people, and, "only if we fully grasp [the concepts of] information, data, systems analysis, and decision modeling, can we truly possess 'foresight and sagacity', and generate the courage and a bold vision consistent with the flow of history. **[4]**

The report further laid out what steps were needed to implement systems engineering in the "social domain". It included, among other things, defining what targets systems management should reach, establishing facilities to ensure information flow, and planning and developing methods and procedures for systems analysis. This explains why systems thinking is key to understanding not only how social credit fits into social management, but overall how the social management system is being designed.

System Construction

Rather than being relatively new conceptions, modern surveillance techniques and social credit are merely the newest developments in realizing the automated social management objective. Advances in AI and big data management further improve their function, from a technical perspective. These advances describe what the Party refers to social management "innovation".

The first major step in the technological development of social management's automation was the implementation of grid management (网格化管理). Structurally, it advanced what has been described as a multilateral "vertical and horizontal integration" (纵横结合) of resources, people and agencies involved in social management. The political-legal and public security apparatus, including neighborhood and street-level committees, largely responsible for the technical side of its day-to-day implementation. Grid management enabled the organization of data to generate better situational awareness and predictive capacity, as well as enhanced tracking and monitoring of individuals (*People's Daily*, October 15, 2006).

The first modern grid(-ized) (网格化) policing was implemented between 2001 and 2002 in cities like Shanghai (*People's Daily* [archive], August 3, 2001; *China File*, August 10, 2016). It organizes information gathering by dividing an urban space into grids, each of these grid spaces is assigned grid managers who help to collect data and pre-empt and solve problems within their grid. The modern informatized grid enables faster emergency response and improved prevention and control. The photographs and videos police take at the scene of almost every protest are one example of the kind of data fed into the grid system.

Grid management's application to social management was significantly expanded between 2002–2012 under the direction of Zhou Yongkang, first as minister of Public Security and later as head of the Central Political-Legal Affairs Committee. Advances in integrated e-government resources in the internal security apparatus, namely the Golden Shield Project, greatly enabled grid management. The Golden Shield

Project is not an internet monitoring project updating the Great Firewall. Rather it is an e-government project creating an organizational network connecting the Ministry of Public Security with its local-level bureaus, which was already being employed at provincial and city levels by 2002 (*China Brief*, June 3, 2011; *People's Daily* [Archive], April 26, 2002). The "Shield" was part of an expanded series of systems engineering projects, originally initiated in 1993 and later expanded as "Golden Projects". Each of the Golden Projects were e-government projects designed to build and streamline information systems, and connect agencies to improve their operational capacity.

This eventually included the multi-phase Golden Shield project, which was being implemented under the guidance of the State Informatization Leading Small Group by the late 1990s and early 2000s. **[5]** For public security bureaus, it improved both efficiency and surveillance. Software applications were developed to integrate data by requiring "real name" registration for travel booking, telecom services, and other services, information from hotel check-in and at customs clearance could be linked to law enforcement databases. The major contribution of the Golden Shield Project to the overall social management program was that it created a capacity to automate information sharing. Ostensibly, the Golden Projects were the technological starting point for building the social credit system, and perhaps social credit was an end goal much earlier in the process. E-government in China has always been designed to improve governance capacity and operate as a feedback loop with social management functions. The timing of social credit implementation probably is explained more by improved technical capacity than by changing policy objectives.

The social credit system relies on the technology enabling and the organizational capacity created through the grid management system. Effectively "social credit" is the technological marriage of individual "responsibility" mechanisms and social control methodologies. Responsibility is a concept underlying the social management process, and it implies that the entire Party and all of society are responsible for upholding the Communist Party's leadership. This is also why individual responsibility is a key theme of all major state security-relevant legislation passed under Xi Jinping (IISS Voices, May 26; *The National Interest*, May 17, 2016). Enabled through the same resources and technology found in grid management, social credit creates a simultaneous co-optative and coercive responsibility systems function, and when fully implemented comprehensively covers all of society. Society is co-opted to participate because the same technology is directly linked to conveniences that improve everyday life, for instance electronic payment. Society is coerced to participate, for instance by self-censoring online, because increasingly technology systems are improving the government's capacity to enforce "responsibility" to the party-state. Not participating could have consequences not only for the individual but also their personal networks. These functions will only become further advanced through plans such as "Internet Plus", as the same technology applications used to provide social and commercial services feed directly into government information gathering and sharing processes (Gov.cn, February 1).

> **Effectively "social credit" is the technological marriage of individual "responsibility" mechanisms and social control methodologies.**

Automated Social Management?

In the construction of the social credit system, current research and development is largely focused on areas such as big data analysis and integration to support the collection of information and ensure its effective use for intelligence. This is one of many areas where advances in artificial intelligence would help streamline social management processes and, perhaps ideally, even automate them. Two major problems, however, confront this automated version of social management.

The first is the struggle for power within the Party. The Party members in charge of day-to-day implementation of social management are also responsible to the Party. As the systems were being enabled in the early 2000s, these agencies had a large amount of relatively unregulated power. The age-old problem of an authoritarian system is that security services require substantial power in order to secure the leadership's authority. The same resources enabling management of the Party-society relationship can be abused by Party members and used against other within the Party (*War on the Rocks*, July 18, 2016). This appears to be the case with Zhou Yongkang, Bo Xilai, and others ahead of the 18th Party Congress. The problem will not disappear in a Leninist system, which not subject to external checks and balances. And it is why ensuring loyalty is a major part of the management of the party side of "state security".

The second probably is a symptom of the first: disaggregated security agencies. In an ideal form, agencies tasked with different aspects of social management can cooperate to address state security problems that have "integrated" characteristics. Usually such threats involve the 'three evil forces' of splittism, terrorism and extremism, and often specifically are related to Tibet, Xinjiang and Falun Gong. Because these are described as threats that have domestic and international connectivity, cooperation between domestic departments, intelligence, and foreign affairs is required for operational success **[6]**. It is particularly applicable in massive multi-agency operations such as "Operation Skynet", tracking down fugitives from the Party-state (*SCMP*, March 26, 2015).

Both problems are explanations for structural changes that put Xi Jinping in charge of leading groups on State Security, Cyber Security, and so on. Using the example of the Central State Security Commission, there are now local government-level iterations in the form of state security work small leading groups in nearly every province, as well as the counties and cities within them. All are led by the relevant party secretary of the locality, and, where data is available, their membership appears to include (but is not limited to) the heads of Political-Legal Affairs Committees, Ministry of State Security bureaus, Armed Police, and Propaganda departments. Similar committees have been set up to mirror other new central leading groups. The membership overlaps significantly. Such leading groups are not new, but the evidence points to the system being utilized not only to re-center power away from the Central Political-Legal Affairs Committee (CPLC) and local versions, but also to develop a more effective system for mobilizing the social management process. For as much as the changes may be geared toward re-centering internal security power, the changes probably serve a dual purpose of creating a capacity for departments to function like a holistic "system of systems". It would address problems by issue—rather than as separate systems addressing overlapping problems.

Conclusion

Chinese information technology research and development, including the priorities outlined in the artificial intelligence plan, are interesting on their own because they mark advances in important research areas. But, as the language of the AI development plan indicates, these advances cannot be separated from Beijing's social management and state security policy. Applied to the social management process, they are aimed at improving governance capacity—automating the "carrot" and "stick" processes that ensure the Party-state's power. Senior CCP leadership hopes that through automation the Party will be able to more effectively anticipate and react to emerging problems, pre-empting a crisis before they become serious threats to stability.

Samantha Hoffman is an independent consultant. She is currently finalizing her Ph.D.: "Programming China: The Communist Party's Autonomic Approach to Managing State Security". She tweets @he_shumei

Notes:

1. A translation of the plan, completed by Graham Webster, Paul Triolo, Elsa Kania and Rogier Creemers, is available at China Copyright and Media blog: https://chinacopyrightandmedia.word-press.com/2017/07/20/a-next-genera-tion-artificial-intelligence-development-plan/

2. Social management (社会管理) and social governance (社会治理) are two phrases that, in practice, have the same definition and are implementing exactly the same process, but the shift from "social management" to "social governance" under Xi Jinping has more to do with political power and ensuring the effectiveness of the social management process, than actual conceptual change. Hoffman, Samantha. "Portents of Change in China's Social Management." *China Brief* 12, no. 15 (2012): pp. 5-8; Hoffman, Samantha, and Peter Mattis. "China's Proposed "State Security Council": Social Governance under Xi Jinping," *China Policy Institute: Analysis,* 21 November 2013. accessed via China Policy Institute.

3. Heath, Timothy. "Xi's Mass Line Campaign: Realigning Party Politics to New Realities." *China Brief* 13, no. 16 (2013): 3-6. Mao, Zedong. "Some Questions Concerning Methods of Leadership " Marx-ists.org, 1 June 1943, https://www.marx-ists.org/reference/archive/mao/selected-works/volume-3/mswv3_13.htm.

4. The People's Daily [archive], September 13, 1984

5. Zhou, Hongren, Hongyuan Xu, Yuxian Zhang, Changsheng Wang, and Xinhong Zhang. *China E-Government Development Report No. 1* (中国电子政务发展报告) *Blue Book of Electronic Development* (电子政务蓝皮书). 2003.

6. UIR Center for International Strategy and Security Studies (中国关系学院国际战略与安全研究中心), *Annual Report on China's National Security Studies 2014* (中国国家安全研究报告 2014), *Blue Book of National Security* (Beijing: Social Sciences Academic Press (China), 2014), p.133.

*** *** ***

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

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

Interested in contributing to China Brief? Read our author guidelines here first.