

CHAPTER 2

CHINA'S IMPACT ON U.S. SECURITY INTERESTS

SECTION 1: MILITARY AND SECURITY YEAR IN REVIEW

Introduction

This section—based on a Commission hearing, discussions with outside experts and U.S. Department of Defense (DoD) officials, and independent research—examines China's late 2012 national and military leadership transition, China's 2012 defense white paper, China's 2013 defense budget, China's military modernization, security developments involving China, and the U.S.-China security relationship. The section concludes with a discussion of China's impact on U.S. security interests. See chapter 2, section 2 and chapter 2, section 3, for coverage of China's cyber activities and China's maritime disputes, respectively.

Leadership Transition

President Xi Jinping Assumes Central Military Commission Chairmanship

China's late 2012 leadership transition brought the largest turnover to the Central Military Commission (CMC)* in a decade. Xi Jinping assumed the position of both CMC chairman and Chinese Communist Party (CCP) general secretary at the CCP's 18th Party Congress on November 15, 2012. President Xi then completed his accession as China's senior leader by becoming the People's Republic of China (PRC) president on March 14, 2013. Although President Xi was widely expected to eventually assume all three of China's top leadership posts, many observers were surprised by the speed of his elevation to CMC chairman. Official Chinese press described President Xi's early promotion as an "unusual twist to China's leadership transition" and praised outgoing CMC Chairman Hu Jintao for his decision to step down.¹ Mr. Hu broke with the pattern established by his two predecessors, who retained the CMC chairmanship for two years after finishing their terms as CCP general secretary.

Cheng Li, director of research and a senior fellow at the Brookings Institution's John L. Thornton China Center, testified to the

*The CMC is China's highest military decision-making body. Its main responsibilities are to set military policy and strategy, interpret Chinese Communist Party guidance for the military, and oversee the People's Liberation Army's senior staff and service arms.

Commission that Mr. Hu's decision to fully cede power signals a strengthening of CCP succession procedures.² In addition, James Mulvenon, vice president of Defense Group Inc.'s Intelligence Division, told the Commission that President Xi's strong and enduring ties with senior military leaders likely contributed to his rapid promotion. President Xi served as an aide to former Defense Minister Geng Biao from 1979 to 1982. He also is the son of Xi Zhongxun, a former Politburo member and revolutionary leader.³

Factional Imbalance Emerges in China's Senior Leadership

During China's 2012 leadership transition, the "elitist coalition" of the CCP prevailed over the "populist coalition" in personnel selections to China's highest decision-making body, securing six of seven seats on the Politburo Standing Committee (PSC).^{*} The elitist coalition, which had been headed by former President Jiang Zemin and is now led by President Xi, mainly consists of the children of Chinese revolutionary leaders and former high-level officials. The populist coalition, which had been headed by Mr. Hu and now is led by current Chinese Premier Li Keqiang, primarily consists of former Chinese Communist Youth League leaders.

Dr. Li testified to the Commission, "Although the CCP monopolizes power in China ... these two coalitions have been competing for power, influence, and control over policy initiatives since the late 1990s ... This dynamic structure of 'one Party, two coalitions' ... has created something approximating a mechanism of checks and balances in the decision making process."⁴ Dr. Li then explained the "landside victory" by Mr. Jiang and President Xi's camp upsets the "roughly equal balance of power between these two coalitions" and signals a "profound change in the power equation." He speculated scandals during the runup to the leadership transition involving two prominent populists—then Chinese Premier Wen Jiabao and then Secretary of the CCP Central Secretariat Ling Jihua—bolstered the elitist coalition's leverage in the PSC personnel negotiations.⁵

The concentration of elitists on the PSC probably strengthens President Xi's ability to pursue his policy agenda and allows Mr. Jiang and his allies to continue to compete for influence. However, Dr. Li stressed, "This does not mean ... the winner now takes all in Chinese elite politics." He explained the "balance between the two camps in the 25-member Politburo, the Secretariat (the organization that handles daily administrative affairs), and the CMC have largely remained intact."⁶ Furthermore, prominent populist coalition leaders are well-positioned for seats on the next PSC in 2017, as five of the seven current PSC members can serve only one term before reaching mandatory retirement age.

^{*}The PSC consists of the CCP's top-ranking leaders and is China's highest decision-making body. The PSC guides and oversees the work of the Politburo.

Since becoming CMC chairman, President Xi has used public speeches and visits to People's Liberation Army (PLA) units to reaffirm China's long-term military modernization goals; emphasize the importance of a strong military to the fulfillment of the "China Dream," his new political slogan and party campaign; and signal his intent to focus on increasing combat readiness and reducing corruption in the PLA.

"*China Dream*": In November 2012, President Xi introduced the "China Dream" concept, which envisions the "great renewal of the Chinese nation" and the advancement of an international system in which China's successful rise provides an attractive alternate political model to Western ones. Achieving the dream means building a "moderately prosperous society" by 2021 and a "modern socialist society that is strong, democratic, cultured, and harmonious" by 2049.⁷ Although President Xi has emphasized that "peaceful development" and a stable regional environment are essential to create the conditions for this vision, he linked its fulfillment to a strong military in a December 2012 speech while aboard a PLA Navy destroyer.⁸ In June 2013, official PLA media explained, "To the armed forces, the China dream is the strong-army dream, the China dream leads the strong-army dream, and the strong-army dream supports the China dream."⁹ According to Daniel Hartnett, research scientist at the CNA Center for Naval Analyses, the PLA's role in the China Dream is a significant and "potentially worrisome development." Mr. Hartnett explained:

[The policy] reflects Xi's attempt to exert his control over the military and establish a break between himself and his predecessors. It also provides further justification for resources for PLA modernization in any internal 'guns versus butter' debate among China's leadership ... It may also signify a harder turn in China's military policy under Xi. If the PLA is being required to improve its combat capabilities in response to changes in China's security environment, it could indicate that the Chinese leadership increasingly feels that it may have to resort to force to counter what it sees as growing national security concerns.¹⁰

Combat readiness: During his first reported visit to a PLA base as CMC chairman in December 2012, President Xi called for the PLA to increase "combat readiness" through "realistic training."¹¹ Combat readiness has been a central theme of subsequent speeches to the military by President Xi and now features prominently in official PLA statements and documents. For example, official PLA media in January 2013 said the military needs to prevent and overcome the "harmful" practice of training "for show."¹² Furthermore, describing the PLA's 2013 training priorities, Xiao Yunhong, deputy director of the PLA's General Staff Department Military Training Department, said: "The 'scent of gunpowder' in the 'fighting' will be stronger. The entire military will make 'training like real war' ... the main theme of the entire year's training, powerfully strengthening training of mission topics, ensuring that as soon as there is a situation, the military will be able to go forward and fight to victory."¹³

As part of its effort to strengthen realism in training, the PLA in January 2013 announced it had designated a mechanized infantry brigade in the Beijing Military Region as its first dedicated “blue force” unit. The brigade is charged with simulating the “combat methods and tactics” of foreign forces during PLA training and exercises, according to official PLA media.¹⁴ The PLA has used “blue force” units in training since the 1980s,* but previously these units served on only a temporary basis and so did not have sufficient time to learn foreign combat methods and tactics. This new brigade is headquartered in northern China at Zhurihe Training Base, the PLA’s largest training center and experimental site for joint operations and “informationized”† warfare. Official Chinese media explained the blue force brigade has “carefully selected classic cases of local warfare around the world in recent years, devoted itself to studying the advanced operational styles of foreign armed forces, and even [simulated] the armed forces . . . exactly in terms of personnel organization and issuance of oral commands.”¹⁵

Corruption: In a meeting shortly after becoming the CMC chairman, President Xi urged senior PLA officers “to take a firm stand against corruption” and to maintain a “strict work style” and “iron discipline.”¹⁶ Since then, reducing corruption and waste in the PLA has been one of President Xi’s most consistent messages in his public speeches to the military. In addition to rhetoric, President Xi has announced stronger anticorruption regulations for the PLA, including restrictions on military personnel holding banquets, drinking excessive alcohol, and using luxury hotels.

President Xi’s focus on combating corruption in the PLA is part of the CCP’s larger national effort to boost its image to mitigate growing public disillusionment with politics and governance in China.¹⁷ He also is attempting to end practices such as paying for promotion and graft, which some observers have suggested reduces the quality of officers, perpetuates opposition to reforms, threatens PLA modernization and readiness, and undermines loyalty to the CCP. In an unusually candid December 2011 speech, PLA Logistics Department Political Commissar General Liu Yuan, son of former Chinese President Liu Shaoqi (1959–1968) and potential friend of President Xi Jinping,¹⁸ reportedly said, “No country can defeat China . . . Only our corruption can destroy us and cause our armed forces to be defeated without fighting.”¹⁹ General Liu in a later speech reportedly explained, “Certain individuals exchange public money, public goods, public office, and public affairs for personal gain, flouting the law and party codes of conduct, even resorting to verbal abuse and threats, clandestine plots and set ups . . . They deploy all of the tricks of the mafia trade within the army itself.”²⁰

Nevertheless, empirical evidence of PLA corruption remains limited. Only two high-profile PLA corruption cases have become

* Official PLA press frequently refer to the U.S. National Training Center at Fort Irwin, California, in discussions about PLA “blue force” training, suggesting U.S. practices may have influenced the PLA’s development and implementation of the concept. PLA officers have visited Fort Irwin to observe U.S. training on at least four occasions (1985, 1994, 1997, and 2011). Shirley Kan, *U.S.-China Military Contacts, Issues for Congress* (Washington, DC: Congressional Research Service, July 30, 2013).

† In Chinese military doctrine, “informationization” refers to the application of advanced information technology to military operations. The PLA views informationization as a required enabler of its goal to be able to win “local wars under informationized conditions.”

known since 2005. Admiral Wang Shouye was sentenced to life in prison in 2006 for embezzling approximately \$20 million. General Gu Junshan was removed from his post in 2012, and the investigation apparently is ongoing.²¹ Both Admiral Wang and General Gu had served as the deputy director of the PLA General Logistics Department, suggesting officers in logistics positions may be more susceptible to corruption, or corruption charges, due to their involvement in infrastructure and natural resources.

Uniformed Members of the Central Military Commission

In the weeks prior to the CCP's 18th Party Congress, seven new uniformed PLA officers were appointed to the CMC. In his testimony to the Commission, Dr. Mulvenon speculated that "some of the choices were short-term compromises," as five of the seven appointees can serve only one term on the CMC before reaching mandatory retirement age. Dr. Mulvenon also noted the elevation of two vice chairmen with strictly operational backgrounds allows China observers to dispense with the popular misconception that one of the positions is set aside for a political officer.²² Roy Kamphausen, senior advisor for political and security affairs at the National Bureau of Asian Research, stressed to the Commission that the PLA remains a "party army"* even without the presence of a political officer in one of the CMC's top positions, because all PLA officers interact extensively with CCP leaders and eventually serve on the CCP Central Committee after joining the CMC.²³

The new uniformed CMC members likely are more professional than previous CMC officers due to their more diverse careers, advanced education, more sophisticated training, and increased exposure to foreign militaries. Their predecessors tended to have specialized careers, less education and training, and limited interactions with foreign militaries outside the Soviet Union. However, because China has not fought a major war since the Sino-Vietnam War in 1979, the new uniformed CMC members have limited combat experience. In contrast, most of their predecessors participated in long and large-scale campaigns during the Chinese Civil War (1946 to 1949) and Korean War (1950 to 1953).²⁴

Figure 1: Members of the 18th Central Military Commission †

<i>CMC Member</i>	<i>Position</i>
Xi Jinping	Chairman
General Fan Changlong*‡	Vice Chairman

*The PLA is the armed branch of the CCP, not the military force of the PRC.

†CMC members are listed according to official protocol order. An asterisk indicates the officer is a new CMC member.

‡General Fan Changlong's promotion to CMC vice chairman surprised many observers. Not only did General Fan have a relatively low public profile until 2012, but also he was promoted from Military Region commander to CMC vice chairman without first serving as a CMC member. General Fan will reach mandatory retirement age at the CCP's 19th Party Congress, so will serve only one term. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of James C. Mulvenon, February 7, 2013.

Figure 1: Members of the 18th Central Military Commission †—Continued

<i>CMC Member</i>	<i>Position</i>
General Xu Qiliang	Vice Chairman
General Chang Wanquan	Minister of National Defense
General Fang Fenghui *	General Staff Department Chief
General Zhang Yang *	General Political Department Director
General Zhao Keshi *	General Logistics Department Director
General Zhang Youxia *	General Armament Department Director
Admiral Wu Shengli §	PLA Navy Commander
General Ma Xiaotian *	PLA Air Force Commander
General Wei Fenghe *	Second Artillery Corps Commander

Source: Open Source Center, *OSC Graphic: Organizational Chart of China's Military Leadership 2013* (Washington, DC: May 22, 2013). OSC ID: CPF2013 0521017002. <http://www.opensource.gov>.

Defense White Paper

In April 2013, China released the latest version of its biennial defense white paper.¶²⁵ This is the first defense white paper published since President Xi became CMC chairman. Although Chinese military leaders likely began to draft the document before President Xi assumed the position, official Chinese press suggests it contains strategic priorities specific to him.²⁶

Unlike previous iterations, which provided a comprehensive overview of Chinese military and security issues, the 2012 defense white paper focuses on a theme—the PLA's growing role in military missions other than war. The current version also is shorter and less formal and ideological than previous ones. Major General Chen Zhou, a senior fellow at the PLA Academy of Military Science and the document's coordinating author, said China in the future plans to alternate between “subject-specific” defense white papers, such as the 2012 iteration, and the traditional “comprehensive” format.²⁷

Official Chinese media hailed the 2012 defense white paper as a milestone in transparency, citing the “declassification” of military details.²⁸ However, most of this was widely-known information that Beijing had never officially acknowledged, such as the designations of Group Armies under the Military Regions and the breakdown of how the PLA distributes personnel among its service arms. Furthermore, as in previous iterations, the 2012 defense white paper offers no substantive information on important defense issues, in-

§ Admiral Wu Shengli, who has served as PLA Navy Commander since 2006 and was a member of the 17th CMC, was widely expected to be elevated to CMC vice chairman or minister of defense. Dr. Mulvenon in his testimony to the Commission speculated Beijing may have considered Admiral Wu's role in leading the PLA Navy's modernization program—a top priority for Beijing—too critical to move him into a different position. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of James C. Mulvenon, February 7, 2013.

¶ Defense white papers—China's most authoritative statements on national security—are published by the State Council's Information Office and approved by the CMC, Ministry of National Defense, and State Council. Beijing primarily uses these documents as a public relations tool to help ease deepening international concern over China's military modernization and answer calls for greater transparency.

cluding the defense budget; nuclear weapons; and the types and numbers of weapon systems already fielded, being developed, or under consideration for acquisition.

Defense Budget

In March 2013, China announced its official defense budget for 2013 rose 10.7 percent in nominal terms to 720.168 billion RMB (approximately \$117.39 billion), signaling the new leadership's support for the PLA's ongoing modernization efforts. This figure represents 5.3 percent of total government outlays²⁹ and approximately 1.3 percent of estimated gross domestic product (GDP).³⁰ China's official annual defense budget now has increased for 22 consecutive years and more than doubled since 2006. Most Western analysts agree Beijing likely will retain the ability—even with slower growth rates of its GDP and government revenue—to fund its ongoing military modernization for at least the near term.³¹

It is difficult to estimate China's actual defense spending due to a number of reasons, including (1) the uncertainty involved in determining how China's purchasing power parity affects the cost of China's foreign military purchases and domestic goods and services and (2) Beijing's omission of major defense-related expenditures—such as purchases of advanced weapons, research and development programs, domestic security spending, and local government support to the PLA—from its official figures. The Institute of International Strategic Studies assesses China's actual defense spending is 40 to 50 percent higher than the official figure.³² DoD estimated China's actual defense spending in 2012 fell between \$135 billion and \$215 billion, which was approximately 20 to 90 percent higher than China's announced defense budget.³³

Military Modernization

Aircraft Carrier Developments

In September 2012, China commissioned its first aircraft carrier, the *Liaoning*, after approximately six years of renovation work on the former Soviet hull and one year of sea trials. China continues to develop a fixed-wing carrier aviation capability, which is necessary for the carrier to perform air defense and offensive strike missions. The PLA Navy conducted its first successful carrier-based takeoff and landing with the Jian-15 (J-15) in November 2012, certified its first group of aircraft carrier pilots and landing signal officers on the carrier's first operational deployment from June to July 2013, and verified the flight deck operations process in September 2013.³⁴ The PLA Navy will continue to conduct short deployments and shipboard aviation training until 2015 to 2016, when China's first J-15 regiment is expected to become operational.

China plans to follow the *Liaoning* with at least two indigenously built aircraft carriers. The first likely will enter service by 2020 and the second by 2025. As China's aircraft carrier force expands and matures, Beijing will improve its ability to project air power, particularly in the South China Sea, and to perform a range of other missions, such as airborne early warning, antisubmarine warfare, helicopter support to ground forces, humanitarian assistance, search and rescue, and naval presence operations.³⁵

Sea-based Nuclear Deterrent Nears Initial Operational Capability

China's Julang-2 (JL-2) submarine-launched ballistic missile (SLBM) is expected to reach initial operational capability by late 2013.³⁶ The JL-2, when mated with the PLA Navy's JIN-class nuclear ballistic missile submarine (SSBN), will give China its first credible* sea-based nuclear deterrent. The JIN SSBN/JL-2 weapon system will have a range of approximately 4,000 nautical miles (nm), allowing the PLA Navy to target the continental United States from China's littoral waters.³⁷ China has deployed three JIN SSBNs and probably will field two additional units by 2020.³⁸ China also is developing its next generation SSBN, the Type 096,³⁹ which likely will improve the range, mobility, stealth, and lethality of the PLA Navy's nuclear deterrent.

Submarine and Surface Fleets Modernizing and Expanding

The PLA Navy continues to steadily increase its inventory of modern submarines and surface combatants. China is known to be building seven classes of ships simultaneously but may be constructing additional classes.⁴⁰ See figures 2–5 below for more information on PLA Navy orders of battle from 1990 to 2020.

- In 2012, China began building four improved variants of its SHANG-class nuclear attack submarine (SSN). China also continues production of the YUAN-class conventional submarine (SS), some of which include an air-independent propulsion† system that allows for extended duration operations, and the JIN SSBN. Furthermore, China is pursuing two new classes of nuclear submarines—the Type 095 guided-missile attack submarine (SSGN) and the Type 096 SSBN—and may jointly develop four advanced conventional submarines with Russia.⁴¹ The PLA Navy's growing inventory of modern nuclear and conventional submarines will significantly enhance China's ability to strike opposing surface ships throughout the Western Pacific and allow it to protect future sea-based nuclear deterrent patrollers and aircraft carrier task groups.⁴²
- In 2012, China launched two new surface combatants—the LUYANG III-class guided-missile destroyer (DDG) and the JIANGDAO-class corvette—and resumed construction of the LUYANG II-class DDG after a brief hiatus. China also continues serial production of the JIANGKAI II-class guided-missile frigate. Most of these units likely will be operational by 2015. The expanding and modernizing surface force will improve Beijing's ability to project power in the East and South China Seas and the Western Pacific. It also will help the PLA

*The PLA Navy operates one SSBN/SLBM weapon system with the XIA-class SSBN and the JL-1 SLBM. However, the status of this weapon system is unclear, and DoD does not consider it to be a credible threat. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: May 2013), p. 6; U.S. Office of Naval Intelligence, *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics* (Suitland, MD: 2009), p. 23.

†Air-independent propulsion (AIP) is a method of generating electrical power in a conventional submarine while it operates submerged. The use of an AIP system reduces the need for a submarine to surface or come to periscope depth—where it is easier to detect—to recharge its batteries.

Navy fulfill its growing set of nontraditional missions beyond China's immediate periphery. These missions include defense of distant maritime trade routes, humanitarian assistance, and counterpiracy.⁴³

- In 2012, the PLA Navy commissioned two YUZHAO-class amphibious transport docks (LPD), bringing its LPD inventory to three. The YUZHAO LPD can carry a mix of air-cushion landing craft, amphibious armored vehicles, helicopters, and marines. This will provide the PLA Navy with additional flexibility while performing missions such as amphibious assault, humanitarian assistance, and counterpiracy and improve China's ability to seize and hold Taiwan's offshore islands. China may build additional YUZHAO LPDs and probably will field a new landing helicopter assault ship, called the Type 081, by 2018.⁴⁴
- In 2013, China added two upgraded FUCHI-class auxiliary replenishment oilers (AOR) to its fleet, raising its number of AORs from five to seven. The increased number of naval support ships better equips the PLA Navy's surface fleet, including future aircraft carrier task groups and expeditionary forces, to sustain high-tempo operations at longer ranges.⁴⁵

According to Chinese military experts Andrew Erickson and Gabe Collins, "by 2015, China will likely be second globally in numbers of large warships built and commissioned since the Cold War's end ... by 2020, barring a U.S. naval renaissance, it is possible that China will become the world's leading military shipbuilder in terms of numbers of submarines, surface combatants and other naval surface vessels produced per year."⁴⁶ The Office of Naval Intelligence projects China will have between 313 and 342 submarines and surface combatants by 2020, including approximately 60 submarines that are able to employ submarine-launched intercontinental ballistic missiles or antiship cruise missiles and approximately 75 surface combatants that are able to conduct multiple missions or that have been extensively upgraded since 1992.⁴⁷

Figure 2: PLA Navy Submarine Orders-of-Battle 1990–2020

Type	1990	1995	2000	2005	2010	2015	2020
Diesel Attack	88	43	60	51	54	57–62	59–64
Nuclear Attack	4	5	5	6	6	6–8	6–9
Nuclear Ballistic	1	1	1	2	3	3–5	4–5
Total	93	49	66	59	63	66–75	69–78

Sources: Numbers from 1990 to 1995 are based on information from various editions of the International Institute for Strategic Studies' *The Military Balance* series, reprinted in Anthony H. Cordesman et al., *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, DC: Center for Strategic and International Studies, 2013), pp. 157–163. Numbers from 2000 to 2010 and projections for 2015 and 2020 were provided by the U.S. Office of Naval Intelligence. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

Figure 3: PLA Navy Submarine Orders-of-Battle 1990–2020, Approximate Percent Modern *

Type	1990	1995	2000	2005	2010	2015	2020
Diesel Attack	0%	0%	7%	40%	50%	70%	75%
Nuclear Attack	0%	0%	0%	33%	33%	70%	100%

Sources: Approximate percentages from 1990 to 1995 are based on information from various editions of the International Institute for Strategic Studies' *The Military Balance* series, reprinted in Anthony H. Cordesman et al., *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, DC: Center for Strategic and International Studies, 2013), pp. 157–163. Approximate percentages from 2000 to 2010 and projections for 2015 and 2020 were provided by the U.S. Office of Naval Intelligence. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

Figure 4: PLA Navy Surface Orders-of-Battle 1990–2020 †

Type	1990	1995	2000	2005	2010	2015	2020
Aircraft Carriers	0	0	0	0	0	1	1–2
Destroyers	19	18	21	21	25	28–32	30–34
Frigates	37	37	37	43	49	52–56	54–58
Corvettes	0	0	0	0	0	20–25	24–30
Amphibious Ships	58	50	60	43	55	53–55	50–55
Coastal Patrol (Missile)	215	217	100	51	85	85	85
Total	329	322	218	158	214	239–254	244–264

Sources: Numbers from 1990 to 1995 are based on information from various editions of the International Institute for Strategic Studies' *The Military Balance* series, reprinted in Anthony H. Cordesman et al., *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, D.C: Center for Strategic and International Studies, 2013), pp. 157–163. Numbers from 2000 to 2010 and projections for 2015 and 2020 were provided by the U.S. Office of Naval Intelligence. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

Figure 5: PLA Navy Surface Orders-of-Battle 1990–2020, Approximate Percent Modern ‡

Type	1990	1995	2000	2005	2010	2015	2020
Destroyers	0%	5%	20%	40%	50%	70%	85%
Frigates	0%	8%	25%	35%	45%	70%	85%

Sources: Approximate percentages from 1990 to 1995 are based on information from various editions of the International Institute for Strategic Studies' *The Military Balance* series, reprinted in Anthony H. Cordesman et al., *Chinese Military Modernization and Force Development: A Western Perspective* (Washington, D.C: Center for Strategic and International Studies, 2013), pp. 157–163. Approximate percentages from 2000 to 2010 and projections for 2015 and 2020 were provided by the U.S. Office of Naval Intelligence. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

* Modern submarines are those able to employ submarine-launched intercontinental ballistic missiles or antiship cruise missiles. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

† Totals do not include all types and sizes of surface ships, such as mine warfare and auxiliary ships.

‡ Modern surface ships are those able to conduct multiple missions or that have been extensively upgraded since 1992. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.

Sustaining the U.S. Military’s “Rebalance” to Asia

In June 2010, then U.S. Secretary of Defense Robert Gates announced the “U.S. defense posture in Asia is shifting to one that is more geographically distributed, operationally resilient, and politically sustainable.”⁴⁸ In January 2012, DoD’s *Defense Strategic Guidance* declared the U.S. military will “of necessity rebalance toward the Asia” by emphasizing existing alliances, expanding its networks of cooperation with “emerging” partners, and investing in military capabilities to ensure access to and freedom to maneuver within the region.⁴⁹ The rebalance is a whole-of-government effort that also includes diplomacy, trade, and development.

However, there is growing concern in the United States and among U.S. allies and partners that DoD will be unable to follow through on its commitment to the rebalance due to declining defense budgets and emerging crises elsewhere in the world. U.S. Defense Secretary Chuck Hagel in July 2013 said Washington would have to choose between a smaller, modern military and a larger, older one if sequester-level funding continues.

In the first approach, we would trade away size for high-end capability. This would further shrink the active Army [from 570,000]⁵⁰ to between 380,000 to 450,000 troops, reduce the number of carrier strike groups from 11 to 8 or 9, draw down the Marine Corps from 182,000 to between 150,000 and 175,000, and retire older Air Force bombers. We would protect investments to counter anti-access and area denial threats, such as the long-range strike family of systems, submarine cruise missile upgrades, and the Joint Strike Fighter, and we would continue to make cyber capabilities and special operations forces a high priority. This strategic choice would result in a force that would be technologically dominant, but would be much smaller and able to go fewer places and do fewer things, especially if crisis occurred at the same time in different regions of the world.

The second approach would trade away high-end capability for size. We would look to sustain our capacity for regional power projection and presence by making more limited cuts to ground forces, ships, and aircraft. But we would cancel or curtail many modernization programs, slow the growth of cyber enhancements, and reduce special operations forces. Cuts on this scale would, in effect, be a decade-long modernization holiday. The military could find its equipment and weapons systems—many of which are already near the end of their service lives—less effective against more technologically advanced adversaries.⁵¹

U.S. Chief of Naval Operations Admiral Jonathan Greenert explained the U.S. Navy’s role in the rebalance: “as directed by the 2012 *Defense Strategic Guidance* . . . the [U.S.] Navy formulated and implemented a plan to rebalance our forces, their homeports, our capabilities, and our intellectual capital and partnerships toward the Asia Pacific.”⁵² Specifically, the U.S. Navy

**Sustaining the U.S. Military’s “Rebalance” to Asia—
Continued**

aims to increase its presence in the Asia Pacific from about 50 ships in 2013 to 60 ships by 2020 and “rebalance homeports to 60 percent” in the region by 2020.⁵³ However, Admiral Greenert has warned constraints in the current budget environment could delay or prevent the U.S. Navy from achieving these objectives. In a September 2013 hearing held by the U.S. House Committee on Armed Services, Admiral Greenert testified:

... If fiscally constrained to the revised discretionary caps, over the long term (2013–2023), the Navy of 2020 would not be able to execute the missions described in the [Defense Strategic Guidance] ... One potential fiscal and programmatic scenario would result in a ‘2020 Fleet’ of about 255–260 ships, about 30 less than today, and about 40 less than the [U.S. Navy’s 2014 budget] submission. It would include 1–2 fewer [carrier strike groups], and 1–2 fewer [amphibious readiness groups] than today. With regard to the [Defense Strategic Guidance] and presence, in this particular scenario the ‘2020 Fleet’ would not increase presence in the Asia-Pacific, which would stay at about 50 ships in 2020. This would largely negate the ship force structure portion of [the U.S.] plan to rebalance to the Asia Pacific region directed by the [Defense Strategic Guidance] ... Overall, in this scenario, development of our capabilities to project power would not stay ahead of potential adversaries’ [anti-access/area denial] capabilities.⁵⁴

Developing Sea-based Land Attack Capability

China currently does not have the ability to strike land targets with sea-based cruise missiles. However, the PLA Navy likely is developing a land attack capability for its Type-095 SSGN and LUYANG III DDG. Modern submarines and surface combatants equipped with land attack cruise missiles (LACMs) will complement the PLA’s growing inventory of air- and ground-based LACMs and ballistic missiles, enhancing Beijing’s flexibility for attacking land targets throughout the Western Pacific, including U.S. facilities in Guam.⁵⁵

Antiship Ballistic Missile Update

In 2010, China deployed the Dong Feng-21D (DF-21D) antiship ballistic missile (ASBM). The DF-21D, which has a range exceeding 810 nm, provides Beijing with the ability to threaten large surface ships, such as U.S. Navy aircraft carriers, throughout the Western Pacific. China is fielding additional DF-21D missiles and may be developing a longer-range variant.⁵⁶

Possible Test of New Antisatellite Capability

On May 13, 2013, China fired a missile into space from the Xichang Satellite Launch Center in western China.* The missile “appeared to be on a ballistic trajectory to nearly geosynchronous Earth orbit,” according to DoD.† Geosynchronous Earth orbit can be achieved at about 22,000 to 23,000 miles above the Earth’s equator.‡ This launch is the world’s highest known suborbital launch since the U.S. Gravity Probe A in 1976 and China’s highest known suborbital launch to date, according to Jonathan McDowell, a scientist at the Harvard-Smithsonian Center for Astrophysics.⁵⁷

U.S. defense agencies reportedly assess the launch was the first test of a new antisatellite (ASAT) capability, according to two U.S. press reports citing unnamed U.S. officials.⁵⁸ Beijing, however, claims the launch was part of a high-altitude scientific experiment for China’s National Space Science Center. A Chinese Ministry of Foreign Affairs spokesperson said he was “not aware” of an ASAT test and then reiterated China’s “longstanding stance to make peaceful use of the outer space and oppose weaponization and arms race in the outer space.”⁵⁹ DoD did not comment on the U.S. press reports or provide information on its assessment of the relationship between the May missile launch and China’s ASAT program.

Although it is difficult to draw a definitive conclusion about the nature of the missile launch without more information from China or DoD, available data suggest it was intended to test at least the launch vehicle component of a new high-altitude ASAT capability.⁶⁰ If the launch is part of China’s ASAT program, Beijing’s attempt to disguise it as a scientific experiment would demonstrate a lack of transparency about its objectives and activities in space. Furthermore, such a test would signal China’s intent to develop an ASAT capability to target satellites in an altitude range that includes U.S. Global Positioning System (GPS) and many U.S. military and intelligence satellites.§ In a potential conflict, this capability could allow China to threaten the U.S. military’s ability to detect foreign missiles and provide secure communications, naviga-

*China’s Academy of Sciences National Space Science Center issued the following statement regarding China’s May missile launch: “This test used a high altitude space probe rocket, which carried a payload of multiple scientific detectors such as Langmuir probes, high energy particle detectors, magnetometers, and barium powder release test devices, etc. to perform original state detection of high energy particles and electromagnetic field strength in the ionosphere and near earth space.” Xinhua, “China Successfully Carries out a High Altitude Scientific Measurement Test,” May 14, 2013. OSC ID: CPP20130514003004.

†DoD issued the following statement regarding China’s May missile launch: “We detected a launch on May 13 from within China. The launch appeared to be on a ballistic trajectory nearly to geosynchronous Earth orbit. We tracked several objects during the flight but did not observe the insertion of any objects into orbit and no objects associated with this launch remain in space. Based upon observations, we assess that the objects reentered the atmosphere above the Indian Ocean. We defer any further questions to the government of China.” Jonathan McDowell, “Kunpeng-7,” *Space Report*, May 21, 2013. <http://www.planet4589.org/pipermail/jsr/2013-May/000051.html>.

‡For an overview of the different classes of orbit, see NASA Earth Observatory, “Three Classes of Orbit.” <http://earthobservatory.nasa.gov/Features/OrbitsCatalog/page2.php>.

§It is not clear from U.S. press reports which type of attack mechanism the potential new ASAT capability would employ. For example, it could use a “kinetic kill vehicle” to disable or destroy a satellite through the force of a direct collision. The new ASAT capability also could employ electronic warfare or directed energy weapons to temporarily degrade a satellite’s capabilities without permanently destroying or damaging it. For an overview of the different types of ASAT attack methods and technologies, see David Wright, Laura Grego, and Lisbeth Gronland, *The Physics of Space Security: A Reference Manual* (Cambridge, MA: American Academy of Arts and Sciences and Union of Concerned Scientists, 2005). <http://www.ucsusa.org/assets/documents/nwgs/physics-space-security.pdf>.

tion, and precision missile guidance. Beijing's January 2007 destruction of an aging Chinese FY-1C weather satellite demonstrated it has the capability to target satellites in low Earth orbit (an altitude between about 100 to 1,200 miles), such as remote sensing satellites.

Developing Operationally Responsive Space Capability

On September 25, 2013, China launched a satellite into space from the Jiuquan Satellite Launch Center in western China. Official Chinese press claims the satellite, carried on a missile called the "Kuaizhou," will "monitor natural disasters and provide disaster relief information" for China's National Remote Sensing Center.⁶¹ However, Gregory Kulacki, China project manager and senior analyst at the Union of Concerned Scientists, explains that, in addition to orbiting a weather satellite, the launch served to test a new solid-fueled launch vehicle. Solid-fueled rockets are simpler to operate, cheaper, and have fewer logistical requirements than liquid-fueled rockets, making them ideal for quick launches with minimal preparation. According to Dr. Kulacki, "This capability would allow [the PLA] to rapidly replace satellites that might be damaged or destroyed in an anti-satellite attack with small but 'good enough' satellites able to restore at least some of the functions of the satellites lost." The U.S. military has been developing a similar capability, which it refers to as "Operationally Responsive Space," since at least 2006.*⁶²

Beidou Regional Satellite Navigation System Complete

On December 27, 2012, China's Beidou regional satellite navigation system † became fully operational and available for commercial use. Using 16 satellites and a network of ground stations, Beidou provides subscribers in Asia with 24-hour precision, navigation, and timing services, as well as the ability to send and receive text messages up to 120 Chinese characters.⁶³ China plans to expand Beidou into a global satellite navigation system by 2020.⁶⁴

China's Satellite Navigation Office emphasized Beidou's importance to the PLA and Chinese commercial interests, stating the system meets the "demands of China's national security, economic development, technological advances and social progress ... safeguard[s] national interests ... enhance[s] the comprehensive national strength ... promote[s] the development of satellite navigation industry ... make[s] contributions to human civilization and social development ... [and] serve[s] the world and benefit[s] mankind."⁶⁵

*DoD's Operationally Responsive Space Office, established in 2007, is charged with planning and preparing "for the rapid development of highly responsive space capabilities that enable delivery of timely warfighting effects and, when directed, develop and support deployment and operations of these capabilities to enhance and assure support to Joint Force Commanders' and other users' needs for on-demand space support, augmentation, and reconstitution." U.S. Operationally Responsive Space Office, *Mission Statement*. <http://ors.csd.disa.mil/mission/>.

† The regional Beidou system, which China refers to as Beidou-2, grew out of an earlier satellite constellation, known as Beidou-1. Beidou-1 provided limited precision, navigation, and timing services in China and a small portion of East Asia but served primarily as a developmental platform for future projects. For more information on China's civilian and military space activities, see U.S.-China Economic and Security Review Commission, *2011 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2011), pp. 198–222.

- Beidou is a critical part of China's stated goal to prepare for fighting wars under "informationized conditions," which includes an emphasis on developing the PLA's C4ISR* and electronic warfare capabilities. The PLA is integrating Beidou into its systems to improve its command and control and long-range precision strike capabilities and to reduce the PLA's reliance on foreign precision, navigation, and timing services, such as GPS.⁶⁶
- Beijing seeks to use Beidou to gain 15–20 percent of China's domestic satellite navigation market share by 2015 and 70–80 percent by 2020. GPS currently has about 95 percent of China's market.⁶⁷
- Beijing is marketing Beidou's services to countries throughout Asia and has already reached agreements with Thailand, Laos, Brunei, and Pakistan to provide precision, navigation, and timing services for government and military customers at heavily subsidized costs.⁶⁸ These agreements include provisions allowing Beijing to build satellite ground stations outside of China, which will be used to increase Beidou's range and signal strength.⁶⁹

Manned Space Program Reaches Milestone

In mid-June 2013, three astronauts aboard China's Shenzhou-10 space shuttle docked with the Tiangong-1, which is a small orbiting experimental space lab that China launched in 2011. Shenzhou-10 was China's fifth manned spaceflight, second manned mission to the Tiangong-1, and longest human spaceflight to date. Over the 15-day mission, the crew conducted both automatic and manual dockings, as well as medical, technological, and scientific experiments while aboard the Tiangong-1.⁷⁰ China's second-ever female astronaut, Wang Yaping, gave a physics lesson from the space lab to more than 60 million Chinese students via live broadcast.⁷¹ President Xi attended the Shenzhou-10 launch and later told the crew in a video conference: "The space dream is a crucial part of our nation-building dream. With the rapid development of China's space industry, a great step forward will be made by the Chinese people in the exploration of space."⁷²

According to Vice Premier Zhang Gaoli, Shenzhou-10's multiple successful dockings with the Tiangong-1 mark the achievement of the second phase of China's three-phase manned space program. In phase one, China launched several unmanned missions to develop technologies necessary for its first manned spaceflight in 2003. In phase two, China honed its spacecraft rendezvous and docking capabilities. In phase three, scheduled for completion by 2023, China plans to launch a permanent manned space station into orbit.⁷³

Official Chinese statements emphasize the civilian aspects of China's space program and only implicitly refer to the PLA's role in China's space strategy. Beijing's 2011 Space White Paper states China's objectives in space are the following:

*C4ISR refers to command, control, communications, computers, intelligence, surveillance, and reconnaissance.

*to explore outer space and to enhance understanding of the Earth and the cosmos; to utilize outer space for peaceful purposes, promote human civilization and social progress, and to benefit the whole of mankind; to meet the demands of economic development, scientific and technological development, national security and social progress; and to improve the scientific and cultural knowledge of the Chinese people, protect China's national rights and interests, and build up its national comprehensive strength.*⁷⁴

However, the PLA has a significant role in most aspects of China's space activities. Scott Pace, director of the Space Policy Institute at George Washington University's Elliott School of International Affairs, testified to the Commission: "China's human space flight efforts are managed by elements of the PLA and require industrial capabilities that are the same as those used for military programs. Thus it might be more accurate to say that China has civil space activities, such as science and exploration, but does not have a civil space program."⁷⁵ This suggests even ostensibly civilian projects, such as the Shenzhou missions and the Tiangong-series space labs, support the development of PLA space, counterspace, and conventional capabilities.

Indigenous Large Transport Aircraft Conducts First Flight Test

In late January 2013, China conducted the first test flight of its indigenously developed cargo transport aircraft, the Yun-20 (Y-20). China previously was unable to build heavy transports, so it has relied on a handful of Russian Ilyushin-76 (Il-76) aircraft for strategic airlift since the 1990s. Following the exposure of key shortcomings in the PLA's ability to conduct disaster relief after China's 2008 Sichuan earthquake, official Chinese media highlighted the PLA's lack of strategic airlift as an "obvious insufficiency" that "affects the overall elevation of [China's] core military capability."⁷⁶

Aircraft specifications provided by official Chinese media indicate the Y-20 can carry about twice the cargo load of the PLA's only operational transport, the Il-76, and about three times the cargo load of the U.S. C-130. Although the Y-20 currently uses Russian engines, the plane's chief designer said China ultimately plans to replace these with Chinese engines that feature better fuel efficiency and thrust-weight ratio.⁷⁷ China also may produce variants of the Y-20 aircraft for specialized missions, such as airborne refueling, airborne early warning, command and control, and electronic warfare.⁷⁸

Once large-scale deliveries of the new plane begin, the Y-20 aircraft will be able to support a variety of domestic and international military operations. The Y-20 will enhance the PLA's ability to respond to internal security crises and border contingencies, support international peacekeeping and humanitarian assistance operations, and project power in a regional conflict.⁷⁹

New Bomber Deployed

In June 2013, the PLA Air Force began to receive new Hongzha-6K (H-6K) bomber aircraft.⁸⁰ The H-6K—an improved variant of

the H-6 (originally adapted from a late-1950s Soviet design)—has extended range and can carry China's new long-range LACM. The bomber/LACM weapon system provides the PLA Air Force with the ability to conduct conventional strikes against regional targets throughout the Western Pacific, including U.S. facilities in Guam.⁸¹ Although the H-6K airframe could be modified to carry a nuclear-tipped air-launched LACM, and China's LACMs likely have the ability to carry a nuclear warhead, there is no evidence to confirm China is deploying nuclear warheads on any of its air-launched LACMs.⁸²

Marketing New Armed Unmanned Aerial Vehicle

At China's major biennial airshow in November 2012, the Chengdu Aircraft Design Institute, which falls under the state-owned Aviation Industry Corporation of China, presented for the first time a static display of the Wing Loong armed unmanned aerial vehicle (UAV).⁸³ The Wing Loong appeared again at the Paris Air Show in June 2013, marking China's first display of an armed UAV at an international defense exhibition.⁸⁴ A representative of China's largest defense aviation exporter at the air show revealed that as many as six countries in Africa and Asia are negotiating with China to purchase the Wing Loong.⁸⁵

Press observers noted the Wing Loong's close resemblance to the MQ-9 Reaper, one of the U.S.'s chief attack UAVs, leading some analysts to speculate Chinese espionage may have contributed to the Wing Loong's development.⁸⁶ Furthermore, U.S. cybersecurity company FireEye in September 2013 exposed an extensive PLA cyber espionage campaign targeting top aerospace and defense firms for information on U.S. drone technology.⁸⁷ FireEye attributed the campaign to a cyber threat group known as "Comment Group," which U.S. cybersecurity company Mandiant has linked to the 2nd Bureau of the PLA General Staff Department's Third Department.⁸⁸ This suggests cyber espionage may have played a role in the new UAV's design. For more information on China's cyber actors and operations, see chapter 2, section 2, of this Report, "China's Cyber Activities."

Security Developments

Expanding Military Operations in Foreign Exclusive Economic Zones

In 2012, the PLA Navy for the first time began to conduct maritime intelligence collection operations in foreign exclusive economic zones (EEZs)* without providing advance notification.⁸⁹ In one instance, the PLA Navy operated near Hawaii during a major U.S.-led multilateral exercise.⁹⁰ This activity runs counter to Beijing's insistence that foreign militaries provide notification and receive approval prior to operating in China's claimed EEZ. In June 2013,

* According to the United Nations Convention on the Law of the Sea, a coastal state is entitled to an EEZ, a 200 nautical mile zone extending from its coastline within which that state can exercise jurisdiction to explore and exploit natural resources, but not full sovereignty.

a senior PLA official confirmed China's naval deployments to foreign EEZs and said China is "sort of reciprocating America's reconnaissance in our EEZ by sending our ships to America's EEZ for reconnaissance." The PLA official added China has done so only "a few times," in contrast to the U.S. and Japan's "almost daily reconnaissance" of China.⁹¹

Although the United States and China agree on the basic role and right of a coastal state to explore, exploit, conserve, and manage natural resources within its EEZ, the two countries have conflicting views on a coastal state's right to regulate foreign military activity in its EEZ, whether they are exercises, military surveys, reconnaissance, or other military operations.⁹² Differences on this issue emerged in the 1970s during United Nations Convention on the Law of the Sea (UNCLOS) negotiations,⁹³ reflecting the contrast in priorities between coastal states with interests in the control and security of their coastal waters and seagoing states with interests in the freedom of the seas. When UNCLOS negotiations concluded in 1982, China was a coastal nation with a littoral navy, whereas the United States was a global maritime power with a blue water navy that operated regularly outside its coastal waters.*

Today, China continues to assert its right to regulate foreign military activities in its claimed EEZ, a minority practice among the world's nations.† China's position is based largely on its view that it has the right to prevent any activity that directly or indirectly threatens its security or economic interests. The United States, maintaining military vessels have high seas freedoms in EEZs, contends China must have due regard for the rights and duties of other states exercising those freedoms in a manner compatible with UNCLOS.⁹⁴ Viewing its own position as one based on international norms, the United States "encourage[s]" similar operations by China, according to U.S. Pacific Command Commander Admiral Samuel Locklear.⁹⁵

China also asserts jurisdiction of its domestic laws in its claimed EEZ. The 1998 *Law of the People's Republic of China on the Exclusive Economic Zone and Continental Shelf* requires foreign entities to obtain Chinese government approval prior to conducting fishing, natural resource exploitation, and marine scientific research in China's claimed EEZ.⁹⁶ China classifies U.S. military and hydrographic surveys as marine scientific research falling under the jurisdiction of this law.‡ The United States considers both types of survey high seas freedoms.

The different interpretations of maritime rights and freedoms in the past decade have led to bilateral tensions and occasionally incidents between U.S. and Chinese maritime and air forces.

*China ratified UNCLOS in 1996. Although the United States has not ratified UNCLOS, it contends the binding principles of UNCLOS conform to customary international law.

†According to the U.S. Navy, only 27 countries share this view, including China, Bangladesh, Burma, Cambodia, India, Malaysia, Maldives, North Korea, Pakistan, Sri Lanka, Thailand, and Vietnam. Ronald O'Rourke, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress* (Washington, DC: Congressional Research Service, April 2013), p. 4.

‡UNCLOS also addresses marine scientific research in the EEZ and continental shelf. United Nations Convention on the Law of the Sea, "Article 246: Marine scientific research in the exclusive economic zone and on the continental shelf." http://www.un.org/depts/los/convention_agreements/texts/unclos/part13.htm; U.S.-China Economic and Security Review Commission, *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2008), pp. 143–147.

One Chinese scholar has suggested the PLA's acknowledgement of its foreign EEZ operations demonstrates that Beijing's "changing concept of maritime affairs" is "moving [China] towards international norms."⁹⁷ Nevertheless, it is unlikely China will completely abandon its existing policy on military activities in EEZs, as doing so would undermine the legal foundation it has sought to build over time as an objector to the international norm. Therefore, in order to avoid being accused of holding contradictory positions, as well as to manage regional perception of its expanding naval activity, Beijing probably will seek to justify its activities using some of the following approaches:

- Continue to rely on domestic law to legitimize a coastal state's authority to regulate foreign military activities in its EEZ. Under this view, which is at odds with state practice by an overwhelming majority of the world's nations, the PLA could justify operating in foreign EEZs absent a coastal state's legislation addressing this matter.
- Seek to distinguish U.S. activity from its own by continuing to classify U.S. operations as marine scientific research that requires coastal state approval.
- Differentiate between U.S. activity off the coast of the Chinese mainland and Chinese operations along the outer reaches of the U.S. geographic periphery.
- Portray such Chinese operations as mere reciprocation of similar U.S. activities.
- Contrast China's less frequent operations with what it describes as the U.S.'s "almost daily reconnaissance."⁹⁸

First Deployment of Infantry to Support UN Peacekeeping Operation

In July 2013, the PLA began to deploy its first peacekeepers to the UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA).⁹⁹ The PLA contingent, which together consists of nearly 400 troops that were dispatched in two groups, includes what Beijing calls a "security force" from the PLA's 16th Group Army.¹⁰⁰ This marks the first time Beijing has deployed infantry to support a peacekeeping operation since it began participating in UN missions in 1990.¹⁰¹ The PLA's security force in Mali is responsible for providing force protection for "MINUSMA headquarters and the living areas of peacekeeping forces."¹⁰² China previously had limited the PLA's participation † in peacekeeping operations to noncombat troops—mainly military observers; staff officers; and engineering, medical, and transportation personnel. For example, China in January 2012 deployed a "guard" unit—consisting of

*MINUSMA took over peacekeeping responsibilities from the African-led International Support Mission in Mali (AFISMA) on July 1, 2013. AFISMA had been providing security since January 2013 when Islamic rebels were ousted from the country. United Nations, *MINUSMA: United Nations Stabilization Mission in Mali*. <http://www.un.org/en/peacekeeping/missions/minusma/background.shtml>.

† Since 2004, China has been contributing police units to UN missions. However, these police units consist of civilians—usually drawn from provincial-level border police units—and are not under the command of the PLA. Bates Gill and Chin-Hao Huang, *China's Expanding Role in Peacekeeping: Prospects and Policy Implications* (Stockholm, Sweden: Stockholm International Peace Research Institute, November 2009), p. 8.

about 50 PLA troops—to the UN Mission in South Sudan.¹⁰³ However, the unit's mission was limited to protecting China's own non-combat troops. Beijing explained the guards were needed because the United Nations was not providing protection for Chinese peacekeepers.¹⁰⁴

Official Chinese statements have downplayed the PLA's deployment of infantry to Mali, likely to avoid raising international concerns about Beijing's intentions and the PLA's growing military capabilities. These statements also have emphasized that China's participation in MINUSMA is consistent with its long-espoused non-interference policy, because Mali requested military assistance. Beijing distinguishes between international action requested by a sovereign state and international action it perceives as designed to overthrow a sovereign state. Beijing fears the latter could legitimize regime change and external intervention and thus threaten China's own core interests of sovereignty and territorial integrity.

China and Russia Hold Large Naval Exercise

In early July, the PLA Navy and the Russian Federation Navy held "Joint Sea-2013" in the Sea of Japan, outside of Vladivostok, Russia. Seven PLA Navy ships—six modern surface combatants and a replenishment ship—participated in the exercise, which included training for antisubmarine operations, antisurface operations, air defense, replenishment at sea, counterpiracy, and search and rescue and concluded with a maritime parade. Official Chinese media highlighted Joint Sea-2013 as the largest deployment of Chinese forces in any joint foreign exercise and the first time the PLA Navy has participated in an "overseas joint exercise far away from [a] naval base and without [a] support system."¹⁰⁵

China and Russia have conducted military drills bilaterally or under the auspices of the Shanghai Cooperation Organization since 2005, but this was only the second naval exercise between the two countries. The first exercise occurred in April 2012 in the Yellow Sea. According to a PLA Navy official, "From now on, the friendly cooperation between Chinese and Russian navies will be further developed, and the exercise will gradually develop towards normalization and institutionalization."¹⁰⁶ Furthermore, during an interview with an official Chinese television station, a Chinese commentator noted, "The antisubmarine subject should be said to be an important subject of this China-Russia joint exercise because antisubmarine exercise has always been a top-secret exercise of various countries ... this shows the military cooperation between the two countries has reached a certain high level of mutual trust."¹⁰⁷

Most Western observers maintain China and Russia are not entering a new stage in security cooperation. Jeffrey Mankoff, a fellow and deputy director of the Russia and Eurasia Program at the Center for Strategic and International Studies, said, "Sporadic cooperation between the Russian and Chinese militaries [does not] alter the fact that China's assertiveness worries Russia at least as much as it worries the United States. Russian military commanders acknowledge that they see China as a potential foe, even as official statements continue to focus on the alleged threat from the United States and [the North Atlantic Treaty Organization]."¹⁰⁸ Furthermore, two of Russia's largest military exercises

since the Soviet era, held in July 2010 and July 2013, focused on its Far East region and were indicative of training for a conflict scenario involving China.¹⁰⁹

Nevertheless, most U.S. observers agree the United States should carefully monitor the status of the China-Russia relationship. Dean Cheng and Ariel Cohen, both senior research fellows at the Heritage Foundation, warned, “If a close Sino–Russian strategic relationship develops, it could limit the capacity of the U.S. to act abroad and undermine economic freedom, democracy, and human rights in Greater Eurasia.”¹¹⁰

China-India Border Tensions Flare

Border tensions between China and India flared after New Delhi claimed a contingent of 30 to 50 PLA soldiers crossed about 12 miles beyond the Line of Actual Control* between the two countries on April 15 and stayed there for three weeks. According to New Delhi, PLA soldiers frequently conduct border incursions (more than 600 times over the last three years) but do not usually cross more than a few miles over the Line of Actual Control nor stay there longer than several hours.¹¹¹

Beijing denied Chinese troops had crossed into Indian territory. A Chinese Ministry of Foreign Affairs spokesperson said, “China has always acted in strict compliance with relevant agreements and protocols between the two countries on maintaining peace and tranquility in the Line of Actual Control area along the border . . . Chinese patrol troops have never crossed the line.”¹¹² Chinese Premier Li Keqiang attempted to downplay the incident and the risk of conflict. During a state visit to India, he insisted that “a few clouds in the sky cannot shut out the brilliant rays of our friendship.” Premier Li did not directly address the alleged Chinese incursion, though he said “both sides believe we need to improve various border-related mechanisms that we have put into place and make them more efficient, and we need to appropriately manage and resolve our differences.”¹¹³

Beijing and New Delhi resolved the April border impasse in May after a series of talks and agreed to pursue a formal agreement to build trust and confidence between the border troops. The two sides signed the agreement during the Indian prime minister’s trip to China in October 2013.¹¹⁴

Nevertheless, the potential for periodic low-level confrontations between border patrols to escalate likely will persist. Indian media have reported several additional albeit briefer incursions by Chinese troops since the April standoff. Furthermore, both China and India continue to boost their militaries’ capabilities on the border, adding to mutual suspicion. This has left both sides sensitive to each other’s border activities and disposed toward worst-case perceptions of the other sides’ intentions and activities. Ely Ratner and Alexander Sullivan of the Center for a New American Security, warn: “more intense strategic competition between India and China would reverberate throughout the continent, exacerbating tensions

*The Line of Actual Control is the effective border between China and India. The 2,400 mile-long Line of Actual Control traverses the Aksai Chin, the northern part of the Sikkim State, and crosses the McMahon Line in Arunachal Pradesh State.

in Central Asia, the Indian Ocean, and Southeast Asia. Disruptions to the Asian engine of economic growth caused by these tensions could debilitate the global economy.”¹¹⁵

“Subtle Shift” in China’s North Korea Policy?

As has been discussed in previous Commission reports, China for decades has provided North Korea with economic and political support and shielded Pyongyang from harsh punishment by the international community for its destabilizing rhetoric and activities.¹¹⁶ However, North Korea’s recent provocations—including its December 2012 long-range rocket launch and February 2013 nuclear test—have led to a “subtle shift” in China’s policy toward North Korea, according to former U.S. Assistant Secretary of State for East Asian and Pacific Affairs Kurt Campbell.¹¹⁷ Observable manifestations of this “subtle shift” are Beijing’s stronger and higher-level public signals of its frustration with Pyongyang. Most notably, President Xi indirectly criticized North Korea in an April speech when he said, “No one should be allowed to throw a region and even the whole world into chaos for selfish gains.”¹¹⁸ This appears to be the first time a Chinese president has publicly reproached North Korea.

Nevertheless, most U.S. analysts agree China has not fundamentally altered its North Korea strategy. Beijing’s recent diplomatic moves have been temporary, limited, easily reversible, and more symbolic than substantive.

- In September 2013, several Chinese government ministries jointly issued a new 236-page list of technologies and materials to be banned from export to North Korea.¹¹⁹ The proscription list focuses on dual-use items that could be used to produce weapons of mass destruction or ballistic missiles. However, according to the Nautilus Institute, “nothing indicates that by issuing tighter controls, China is fundamentally changing its policy toward North Korea, let alone abandoning it . . . The degree to which China enforces the prohibition of trade in items on this list will mostly determine the success of the program.”¹²⁰
- Although China in March 2013 voted to approve new and strengthened UN Security Council sanctions on North Korea,¹²¹ Stephanie Kleine-Ahlbrandt, then North East Asia project director and China adviser for the International Crisis Group, in July noted that China’s implementation of the sanctions had been “underwhelming.”¹²²
- In May 2013, state-owned Bank of China Ltd. closed its account with North Korea’s Foreign Trade Bank. However, Ms. Kleine-Ahlbrandt explains, “It is unclear whether there was any money in the Foreign Trade Bank’s accounts when they were closed. For months already, North Koreans had been limiting their use of major Chinese banks to avoid scrutiny. Third countries are often used for such transactions, as well as provincial Chinese banks, which operate with considerably more autonomy than the larger state-owned banks. Furthermore, most of North Korean trade with China skirts the banking sys-

tem altogether by engaging in cash transactions via trading companies in China, processing payments in the form of gold or gemstones, or even bartering.”¹²³

Joel Wuthnow, analyst at the CNA Center for Naval Analyses, warns: “this refrain is familiar. For instance, China’s harsh rhetoric and vote in favor of UN sanctions after North Korea’s 2006 nuclear test was followed in 2007 by a push for dialogue; a similar pattern developed after China’s approval of sanctions in response to [North Korean] provocations in 2009, with a more conciliatory approach in 2010.”¹²⁴

United States-China Security Relationship

China Seeking “New Type of Major-Country Relationship” with the United States

Throughout 2013, Beijing called for a “new type of major-country relationship”* with the United States. Official Chinese statements claim the “new type” relationship is intended to promote more stable relations between the two countries and avoid or, if necessary, manage tensions that history suggests could occur as China rises. The concept, which was formulated by Beijing in 2011, has been referenced increasingly in official Chinese statements and press since February 2012, when then presumptive Chinese President Xi evoked it during a visit to the United States.¹²⁵ The “new type” relationship was a central theme of the June 2013 summit between President Obama and President Xi in Sunnylands, California.¹²⁶

The “new type” concept, like many Chinese policy slogans, is vaguely defined in order to provide Chinese officials with the flexibility to frame it in different ways for different circumstances and audiences. Chinese officials likely will attempt to use the concept to serve a number of Beijing’s strategic objectives, including the following:

- Develop deeper and more frequent military communication to improve the two countries’ abilities to manage crises if and when they arise.
- Pressure the United States to respect China’s “core interests,” which are to preserve China’s political system and national security, protect Chinese sovereignty and territorial integrity, and sustain economic and social development.
- Promote an image of China as a constructive actor seeking common solutions to regional and global issues.
- Convince the United States that China is proactively seeking to build a peaceful and cooperative bilateral relationship.
- Pressure the United States to cease its military reconnaissance and survey operations in China’s claimed EEZ, reduce U.S. arms sales to Taiwan, and relax restrictions on the military-to-military relationship, particularly those imposed in the 2000 National Defense Authorization Act.[†]¹²⁷

* Chinese statements also use the term “new type of great power relationship.” Both phrases refer to the same concept.

† Section 1201 of the 2000 National Defense Authorization Act prohibits DoD from authorizing any military-to-military exchange or contact with representatives of the PLA if that exchange

Select Military-to-Military Engagements

DoD is seeking to expand and deepen its engagement with the Chinese military in nonsensitive areas of mutual interest. DoD contends a strong military-to-military relationship develops familiarity at the operational level, which reduces the risk of conflict through accidents and miscalculations; builds lines of communication at the strategic level that could be important during a crisis; contributes to better overall bilateral relations; and creates opportunities to obtain greater contributions from China to international security.

From 2012 to 2013, the number of U.S.-China military-to-military contacts—including high-level visits, recurrent exchanges, academic exchanges, functional exchanges, and joint exercises—more than doubled from approximately 20 to 40.¹²⁸ In particular, contact between the U.S. Navy and PLA Navy increased significantly during this timeframe. In July 2013, U.S. Pacific Commander Admiral Locklear said, “I think that the progress that we’re making between our two militaries is quite commendable ... because we are able to have very good dialogue on areas where we converge, and there are a lot of places where we converge as two nations, and we’re also able to directly address in a matter-of-fact way where we diverge.”¹²⁹ Key military-to-military contacts in 2013 include the following:

- In April, U.S. Chairman of the Joint Chiefs of Staff General Martin Dempsey traveled to Beijing to meet with senior Chinese leaders, including President Xi, CMC Vice Chairman General Fan Changlong, and Defense Minister General Chang Wanquan. General Dempsey raised U.S. concerns about Chinese cyber espionage, reiterated U.S. treaty obligations to Japan encompass the Senkaku Islands, and explained the U.S. rebalance to Asia. After the trip, General Dempsey announced both militaries had agreed to a set of joint recommendations for their respective governments, including more frequent and regular military engagements at every level and the development of a code of conduct for interactions in the air, sea, and cyber domains.¹³⁰
- In May, the *USS Shiloh*, a guided-missile cruiser based in Japan, called at Zhanjiang, China, to visit the PLA Navy’s South Sea Fleet headquarters.¹³¹ This marked the first port visit by a U.S. Navy ship to China since 2009.¹³²
- In May, then U.S. Pacific Fleet Commander Admiral Cecil Haney visited Beijing for talks with PLA Deputy Chief of General Staff General Qi Jianguo and PLA Navy Commander Admiral Wu Shengli.¹³³ Admiral Haney then traveled to Zhanjiang to participate in the *USS Shiloh*’s port visit.¹³⁴
- In August, a group of two PLA Navy surface ships and a replenishment ship called at Pearl Harbor, Hawaii. This marked the first port visit by a Chinese ship to the United States since 2006.¹³⁵ The PLA Navy ships then participated in a search and

or contact would create a national security risk for the United States. United States Congress, “National Defense Authorization Act for Fiscal Year 2000,” Public Law 106–65, October 5, 1999. <http://www.gpo.gov/fdsys/pkg/PLAW-106publ65/pdf/PLAW-106publ65.pdf>.

rescue exercise with ships from the U.S. Pacific Fleet. According to U.S. Navy Region Hawaii and Naval Surface Group Middle Pacific Commander Rear Admiral Rick Williams, the exercise included “helicopters working together [for] airspace deconfliction . . . small boat operations back and forth . . . [and] communication drills.”¹³⁶

- In August, the U.S. Fifth Fleet and the PLA Navy conducted the second ever U.S.-China counterpiracy exercise.¹³⁷ A U.S. guided-missile destroyer, a Chinese destroyer, and a Chinese replenishment ship participated in the two-day exercise in the Gulf of Aden. According to DoD press, the drill included “simulated medical emergencies and hostage scenarios . . . a live-fire proficiency exercise . . . [and the] landing of a helicopter from each country aboard the deck of each other’s ships.” Paraphrasing a U.S. Fifth Fleet official, the DoD press report said the exercise marked a “big step forward” from the first U.S.-China counterpiracy exercise in 2012, which “lasted only about six hours and was limited to a basic visit, board, search, and seizure and secure exercise, follow-on discussion, and crew lunch.”¹³⁸
- In August 2013, China’s Defense Minister General Chang Wanquan traveled to the United States, where he visited the U.S. Pacific Command, the U.S. Northern Command, the North American Aerospace Defense Command, and the Pentagon. Defense Minister Chang met with U.S. Secretary of Defense Chuck Hagel at the Pentagon to discuss Asian security, U.S.-China cyber issues, and opportunities to enhance U.S.-China military cooperation. During a joint press conference, Secretary Hagel and Defense Minister Chang gave an overview of recent and planned bilateral exercises; announced plans to establish a dialogue between the U.S. Strategic Plans and Policy Directorate of the Joint Chiefs of Staff and the PLA’s new Strategic Planning Department; and said the two sides continue to develop a notification mechanism for major military activities and rules of behavior for military air and naval activities.¹³⁹
- In September, PLA Navy Commander Admiral Wu Shengli and Senior Captain Zhang Shen, the commanding officer of China’s first aircraft carrier, traveled to San Diego, California, and Washington, DC. In San Diego, the PLA Navy delegation met with U.S. Chief of Naval Operations Admiral Jonathan Greenert; toured a NIMITZ-class aircraft carrier and a LOS ANGELES-class attack submarine; embarked on a Littoral Combat Ship at sea; and visited U.S. Marine Corps Base Camp Pendleton. In Washington, DC, the delegation had a series of talks with U.S. Navy leadership at the Pentagon and visited Walter Reed National Military Medical Center.¹⁴⁰

Additionally, China in March accepted the U.S. invitation, first extended by then U.S. Secretary of Defense Leon Panetta in September 2012, to participate in the U.S.-led multilateral Rim of the Pacific (RIMPAC) Exercise near Hawaii in 2014.¹⁴¹ According to U.S. Pacific Command Commander Admiral Samuel Locklear, this

is “a big step for the Chinese military . . . [the] Chinese navy [will] be entering a multinational three-week-long exercise that’s basically run by the U.S. from the 3rd Fleet headquarters.”¹⁴²

Implications for the United States

China’s military modernization presents significant challenges to U.S. security interests in Asia. First and foremost, major elements of this program—such as the DF-21D antiship ballistic missile and increasing numbers of advanced submarines armed with antiship cruise missiles—are designed to restrict U.S. freedom of action throughout the Western Pacific. As the PLA’s anti-access/area denial* capabilities mature, the costs and risks to the United States for intervention in a potential regional conflict involving China will increase.

Furthermore, the PLA’s rapidly advancing regional power projection capabilities enhance Beijing’s ability to use force against Taiwan, Japan, and rival claimants in the South China Sea. This could embolden China to respond militarily to a perceived provocation or to consider preemptive attacks in a crisis involving Taiwan or China’s maritime sovereignty claims. Many of these scenarios could require the U.S. military to protect U.S. regional allies and partners as well as to maintain open and secure access to the air and maritime commons in the Western Pacific.

At the same time, rising unease over both China’s expanding capabilities and increasing assertiveness is driving U.S. allies and partners in Asia to improve their own military forces and strengthen their security relationships with each other. These trends could support U.S. interests by lightening Washington’s operational responsibilities in the region.

Most Asian countries welcomed the U.S. rebalance to Asia when it was announced by the Obama Administration in 2011. The Philippines, for example, is considering granting the United States access to Subic Bay—a former U.S. naval base.† The Philippines Department of Foreign Affairs Visiting Forces Agreement Director said, “As the [United States] begins to implement [the rebalance to Asia], Subic will play an important role because it is one of the important facilities that can service its presence in the Pacific.”¹⁴³ However, there is growing concern among U.S. allies and partners that the United States will be unable to follow through on its commitment to the rebalance due to declining defense budgets and continuing security challenges elsewhere. Furthermore, some regional countries almost certainly began to question the willingness of the United States to restrain China’s increasing assertiveness after China in 2012 gained de facto control of Scarborough Reef, territory also claimed by the Philippines, a U.S. treaty ally. This perception could lead some regional countries to increasingly accom-

* “Anti-access” (A2) actions are those intended to slow deployment of an adversary’s forces into a theater or cause the forces to operate from distances farther from the conflict than they would otherwise prefer. A2 affects movement into theater. “Area denial” (AD) actions are those intended to impede an adversary’s operations within areas where friendly forces cannot or will not prevent access. AD affects movement within theater. U.S. Air-Sea Battle Office, *Air Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges* (Arlington, VA: May 2013), pp. 2–4.

† Subic Bay—a natural harbor that is about 50 miles north of Manila—served as a major U.S. naval base until the early 1990s.

moderate China or pursue military capabilities that could be used offensively or preemptively. Either scenario could undermine U.S. interests in the region.

Conclusions

- PLA modernization is altering the security balance in the Asia Pacific, challenging decades of U.S. military preeminence in the region.
- The PLA Navy is in the midst of an impressive modernization program. China's acquisition of naval platforms, weapons, and systems has emphasized qualitative improvements, not quantitative growth, and is centered on improving its ability to strike opposing ships at sea and operate at greater distances from the Chinese mainland. Today, the PLA Navy is able to conduct high-intensity operations in China's immediate periphery as well as low-intensity operations beyond the region. Trends in China's defense spending, research and development, and shipbuilding suggest the PLA Navy will continue to modernize. By 2020, China could have approximately 60 submarines that are able to employ submarine-launched intercontinental ballistic missiles or anti-ship cruise missiles and approximately 75 surface combatants that are able to conduct multiple missions or that have been extensively upgraded since 1992.
- The PLA is rapidly expanding and diversifying its ability to strike U.S. bases, ships, and aircraft throughout the Asia Pacific region, including those that it previously could not reach, such as U.S. military facilities on Guam.
- The PLA's expanding involvement in real world missions allows it to field-test equipment and obtain hands-on experience in areas such as addressing unconventional threats in harsh and potentially hostile environments, satisfying expeditionary logistics requirements, and integrating into multilateral operations.
- The PLA is improving its day-to-day readiness levels and conducting longer-range and more frequent, robust, and realistic training. As these reforms continue, the PLA will become more proficient and confident operating its advanced platforms and weapon systems and better able to rapidly respond to regional contingencies.
- The PLA Navy's growing presence in foreign EEZs contradicts its longstanding policy on military activities in its own EEZ. Rather than resolve this inconsistency between its actions and policy, Beijing likely will continue to assert its authority to regulate U.S. military activities in its EEZ.

ENDNOTES FOR SECTION 1

1. Yan Hao, "Xinhua Insight: Hu praised for voluntarily resigning from top post," Xinhua, November 17, 2012. http://news.xinhuanet.com/english/special/18cpcnc/2012-11/18/c_131981526.htm.
2. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Cheng Li, February 7, 2013.
3. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of James C. Mulvenon, February 7, 2013.
4. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Cheng Li, February 7, 2013.
5. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Cheng Li, February 7, 2013.
6. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Cheng Li, February 7, 2013.
7. Xinhua, "Xi pledges 'great renewal of Chinese nation,'" November 29, 2012. http://news.xinhuanet.com/english/china/2012-11/29/c_132008231.htm.
8. Jeremy Page, "For Xi, a 'China Dream' of Military Power," *Wall Street Journal*, March 13, 2013. <http://online.wsj.com/article/SB10001424127887324128504578348774040546346.html>.
9. Xie Zhengxuan, "Basic Adherences that Lead National Defense Construction and Army Building," *Jiefangjun Bao* (PLA Daily), June 15, 2013. OSC ID: CPP20130620088001. <http://www.opensource.gov>.
10. Daniel Hartnett, "Army Day Coverage Stresses Winning Battles with 'Dream of a Strong Military,'" *China Brief* 13:17 (Washington, DC: Jamestown Foundation, August 23, 2013). http://www.jamestown.org/uploads/media/China_Brief_Vol_13_Issue_04.pdf.
11. Cary Huang, "Xi Jinping orders PLA to step up its 'real combat' awareness," *South China Morning Post* (Hong Kong), December 13, 2012. <http://www.scmp.com/news/china/article/1103957/xi-jinping-orders-pla-step-its-real-combat-awareness>.
12. *Jiefangjun Bao* (PLA Daily), "JFJB Commentator on PLA Military Training Directive for 2013," January 14, 2013. OSC ID: CPP20130114787021. <http://www.opensource.gov>.
13. CCTV-7, "Deputy Training Chief Discusses PLA 2013 Military Training Plans," December 28, 2012. OSC ID: CPP20130105678001. <http://www.opensource.gov>.
14. CCTV-7, "The PLA's New Specialized 'Blue Force' Brigade Unveiled in Zhurihe," January 13, 2013. OSC ID: CPP20130122075005. <http://www.opensource.gov>.
15. CCTV-7, "The PLA's New Specialized 'Blue Force' Brigade Unveiled in Zhurihe," January 13, 2013. OSC ID: CPP20130122075005. <http://www.opensource.gov>.
16. Open Source Center, *PRC Media Portray Xi Jinping as Actively Managing Military* (Washington, DC: June 6, 2013). OSC ID: CPP20130606790021. <http://www.opensource.gov>.
17. Willy Lam, "Commander-in-Chief Xi Jinping Raises the Bar on PLA 'Combat Readiness,'" *China Brief* 13:2 (Washington, DC: Jamestown Foundation, January 18, 2013). [http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews\[tt_news\]=40329&cHash=d7a108eeb831585907e389ed5a637ada](http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=40329&cHash=d7a108eeb831585907e389ed5a637ada).
18. James Mulvenon and Leigh Ann Ragland, "Liu Yuan: Archetype of a 'Xi Jinping Man' in the PLA," *China Leadership Monitor* No. 36, January 6, 2012. <http://media.hoover.org/sites/default/files/documents/CLM36JM.pdf>.
19. John Garnaut, "Rotting from Within: Investigating the massive corruption of the Chinese military," *Foreign Policy*, April 16, 2012. http://www.foreignpolicy.com/articles/2012/04/16/rotting_from_within.
20. John Garnaut, "Rotting from Within: Investigating the massive corruption of the Chinese military," *Foreign Policy*, April 16, 2012. http://www.foreignpolicy.com/articles/2012/04/16/rotting_from_within.
21. Wang Xiangwei, "Time for Xi to clean up the sleaze pervading the PLA," *South China Morning Post* (Hong Kong), August 5, 2013. <http://www.scmp.com/news/china/article/1294329/time-xi-clean-sleaze-pervading-pla>.

22. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of James C. Mulvenon, February 7, 2013.

23. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Roy Kamphausen, February 7, 2013.

24. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of James C. Mulvenon, February 7, 2013.

25. Xinhua, "Full Text—The Diversified Employment of China's Armed Forces," April 16, 2013. OSC ID: CPP20130416968060. <http://www.opensource.gov>.

26. Xinhua, "China Voice: Diversified Employment of Armed Forces Guarantees the 'China Dream,'" April 16, 2013. OSC ID: CPP20130416968284. <http://www.opensource.gov>.

27. Luo Zheng, "Provide Strong Support for Our Nation's Peaceful Development—An Interview with Chen Zhou, Director of the National Defense Policy Research Center of the Academy of Military Science," *Jiefangjun Bao* (PLA Daily), April 16, 2013. OSC ID: CPP20130417787007. <http://www.opensource.gov>.

28. Xinhua, "China Declassifies Designations of PLA Corps," April 16, 2013. OSC ID: CPP20130416968122. <http://www.opensource.gov>.

29. Xinhua, "Facts Figures: China's 2013 Draft Budget Report," March 5, 2013. OSC ID: CPP20130305968101. <http://www.opensource.gov>; Bloomberg, "China Boosts Defense Spending as Military Modernizes Arsenal," March 5, 2013. <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>.

30. Luo Zheng, "Investment in Our National Defense Expenditure Mutually Conforms with National Security and Development Interests—Interview with Sun Huangtian, Deputy Director of PLA General Logistics Department, on 2013 National Defense Budget," *Jiefangjun Bao* (PLA Daily), March 6, 2013. OSC ID: CPP20130307088001. <http://www.opensource.gov>; Bloomberg, "China Boosts Defense Spending as Military Modernizes Arsenal," March 5, 2013. <http://www.bloomberg.com/news/2013-03-05/china-boosts-defense-spending-as-military-modernizes-its-arsenal.html>.

31. Adam Liff and Andrew Erickson, "Demystifying China's Defence Spending: Less Mysterious in the Aggregate," *China Quarterly* (2013).

32. The Institute of International Strategic Studies, "China's defence spending: new questions," *Strategic Comments*, August 2, 2013. <http://www.iiss.org/en/publications/strategic%20comments/sections/2013-a8b5/china—39-s-defence-spending—new-questions-e625>.

33. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), p. 45.

34. *Renmin Ribao* (People's Daily), "Chinese aircraft carrier returns to home port," September 22, 2013. <http://english.peopledaily.com.cn/90786/8407244.html>; Xinhua, "China's carrier-borne jet pilots receive certification," July 4, 2013. <http://english.peopledaily.com.cn/90786/8310416.html>; Xinhua, "China's first aircraft carrier leaves homeport for sea trials," June 11, 2013. http://news.xinhuanet.com/english/china/2013-06/11/c_132447284.htm; Xinhua, "China's aircraft carrier anchors in military port," February 27, 2013. http://www.china.org.cn/china/NPC_CPPCC_2013/2013-02/27/content_28071340.htm; and Xinhua, "China Now Capable to Deploy Jets on Aircraft Carrier: Navy," November 25, 2012. OSC ID: CPP20121125968098. <http://www.opensource.gov>.

35. Daniel Kostecka, "From the Sea: PLA Doctrine and the Employment of Sea-Based Airpower," *Naval War College Review* (Newport, RI: Naval War College, July 2011).

36. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), p. 31.

37. U.S. Office of Naval Intelligence, *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics* (Suitland, MD: 2009), p. 23.

38. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 10, 31.

39. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), p. 6.

40. Andrew Erickson and Gabe Collins, "China Carrier Demo Module Highlights Surging Navy," *National Interest*, August 6, 2013. <http://nationalinterest.org/commentary/china-carrier-demo-module-highlights-surg-ing-navy-8842>; U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013; and U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 5–7.
41. BBC, "China 'Buys Fighter Jets and Submarines from Russia,'" March 25, 2013. <http://www.bbc.co.uk/news/world-asia-21930280>; Robert Foster, "Russia to Sell, Co-Produce Lada-class Submarines to China," *IHS Jane's Defence Industry*, December 20, 2012. <http://www.janes.com/article/19682/russia-to-sell-co-produce-lada-class-submarines-to-china>.
42. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 5–7.
43. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 5–7.
44. Ronald O'Rourke, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress* (Washington, DC: Congressional Research Service, July 5, 2013), pp. 33–37; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 7–8, 39.
45. Xinhua, "Meimei: Xin bujijian tigao Zhongguo Haijun zuozhan nengli" (U.S. media source: New supply ship improves Chinese navy's warfighting ability), July 2, 2013. http://news.xinhuanet.com/world/2013-07/02/c_124940680.htm; David Lague, "Chinese transport 'workhorses' extending military's reach," Reuters, February 25, 2013. <http://www.reuters.com/article/2013/02/25/us-china-military-ships-idUSBRE91O15V20130225>; David Axe, "This Simple Ship Could Let the Chinese Navy Circle the Globe," *Wired*, January 16, 2013. <http://www.wired.com/dangerroom/2013/01/china-new-oiler/>; and Christopher D. Yung and Ross Rustici, *China's Out of Area Naval Operations* (Washington, DC: National Defense University, December 2010).
46. Andrew Erickson and Gabe Collins, "China Carrier Demo Module Highlights Surging Navy," *National Interest*, August 6, 2013. <http://nationalinterest.org/commentary/china-carrier-demo-module-highlights-surg-ing-navy-8842>.
47. U.S. Office of Naval Intelligence, *PLA Navy Orders of Battle 2000–2020*, written response to request for information provided to the U.S.-China Economic and Security Review Commission, Suitland, MD, June 24, 2013.
48. U.S. Department of Defense, *Remarks as Delivered by Secretary of Defense Robert M. Gates, Shangri-La Hotel, Singapore* (Washington, DC: June 5, 2010). <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1483>.
49. U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Leadership* (Washington, DC: January 2012). http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.
50. U.S. Department of Defense, *Army Announces Force Structure and Stationing Decisions* (Washington, DC: June 25, 2013). <http://www.defense.gov/releases/release.aspx?releaseid=16114>.
51. U.S. Department of Defense, *Statement on Strategic Choices and Management Review, Pentagon press briefing remarks by Secretary of Defense Chuck Hagel* (Washington, DC: July 31, 2013). <http://www.defense.gov/speeches/speech.aspx?speechid=1798>.
52. Jonathan Greenert, "Foreword," in *U.S. Navy Program Guide 2013* (Washington, DC: 2013). <http://www.navy.mil/navydata/policy/seapower/npg13/top-npg13.pdf>.
53. U.S. Navy, *U.S. Navy Program Guide 2013* (Washington, DC: 2013). <http://www.navy.mil/navydata/policy/seapower/npg13/top-npg13.pdf>.
54. House Committee on Armed Services, *Hearing on Planning for Sequestration in FY 2014 and Perspectives of the Military Services on the Strategic Choices and Management Review*, 113th Cong., 1st sess., September 18, 2013.
55. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: May 2013), pp. 6–7; J. Michael Cole, "China's Growing Long-Range Strike Capa-

bility.” *Diplomat*, August 13, 2012. <http://thediplomat.com/flashpoints-blog/2012/08/13/chinas-growing-long-range-strike-capability/>.

56. Andrew Erickson, “How China Got There: Beijing’s Unique Path to ASBM Development and Deployment,” *China Brief* 13:12 (Washington, DC: Jamestown Foundation, June 7, 2013). http://www.jamestown.org/programs/chinabrief/single?tx_ttnews%5d=40994&tx_ttnews%5bbackPid%5d=25&cHash=913594fd5785c82b653cc6b00de7850c#Ueh_F5U-aX1; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: 2013), pp. 5–6.

57. Jonathan McDowell, e-mail interview with Commission Staff, May 22, 2013; Jonathan McDowell, “Kunpeng-7,” *Space Report*, May 21, 2013. <http://www.planet4589.org/pipermail/jsr/2013-May/000051.html>.

58. Andrea Shalal-Esa, “U.S. sees China launch as a test of anti-satellite muscle: source,” Reuters, May 15, 2013. <http://www.reuters.com/article/2013/05/15/us-china-launch-idUSBRE94E07D20130515>; Bill Gertz, “China Conducts Test of New Anti-Satellite Missile,” *Washington Free Beacon*, May 14, 2013. <http://freebeacon.com/china-conducts-test-of-new-anti-satellite-missile/>.

59. Ministry of Foreign Affairs (China), *Foreign Ministry Spokesperson Hong Lei’s Regular Press Conference on May 14, 2013* (Beijing, China: May 14, 2013). OSC ID: CPP20130515968206. <http://www.opensource.gov>.

60. Andrea Shalal-Esa, “RPT—China’s space activities raising U.S. satellite security concerns,” Reuters, January 14, 2013. <http://www.reuters.com/article/2013/01/14/china-usa-satellites-idUSL2N0AJ10620130114>; Central News Agency (Taipei), “Beijing to Trigger Arms Race by Testing Anti-satellite Missiles,” January 13, 2013. OSC ID: CPP20130115968204. <http://www.opensource.gov>; Gregory Kulacki, “Is January Chinese ASAT Testing Month?” *All Things Nuclear, Insights on Science and Security*, January 4, 2013. <http://allthingsnuclear.org/is-january-chinese-asat-testing-month/>; U.S. Department of Defense, *China: PLA Activities Report 16–31 Oct 2012* (Washington, DC: October 31, 2012). OSC ID: CPP20121120440020. <http://www.opensource.gov>; Xinhua, “China Dismisses Report on Planned Test Launch of Anti-Satellite Missile,” October 25, 2012. OSC ID: CPP20121025968325. <http://www.opensource.gov>; and Bill Gertz, “China to Shoot at High Frontier,” *Washington Free Beacon*, October 16, 2012. <http://freebeacon.com/china-to-shoot-at-high-frontier/>.

61. Xinhua, “China Launches Satellite to Monitor Natural Disaster,” September 25, 2013. http://news.xinhuanet.com/english/china/2013-09/25/c_132749677.htm.

62. Lee Doggrell, “Operationally Responsive Space,” *Air & Space Power Journal* 20:2 (Summer 2006), pp. 42–49. www.dtic.mil/cgi-bin/GetTRDoc?AD=ADP023958.

63. Bingqi Zhishi (Ordnance Knowledge), “Beidou, China’s Pride,” August 1, 2012. OSC ID: CPP20121016680010. <http://www.opensource.gov>.

64. Xinhua, “China Targeting Navigation System’s Global Coverage by 2020,” March 3, 2012. http://news.xinhuanet.com/english/sci/2013-03/03/c_132204892.htm.

65. Satellite Navigation Office (China), *Report on the Development of Beidou Navigation Satellite System* (Beijing, China: December 26, 2012). <http://www.beidou.gov.cn/attach/2012/12/26/20121226d63d5539977a4deab28cebea685ced1a.pdf>.

66. *Jiefangjun Bao* (PLA Daily), “Navy North Sea Fleet’s New Smart Target Ship Emits Electromagnetic Jamming Against Missiles,” August 04, 2013. OSC ID: CHO2013080530196614. <http://www.opensource.gov>; Yu Hu, “PLA Jinan MR Extends Military Use of the Beidou Satellite Navigation System,” *Jinan Qianwei Bao* (Jinan Front News), January 17, 2012. OSC ID: CPP20130222667020. <http://www.opensource.gov>; and Sun Chao, Zhang Jun, and Wang Jun, “PLA Chengdu MR Sichuan Div Uses Satellite Navigation to Standardize Time,” *Chengdu Zhanqi Bao* (Chengdu Battle Standard News), November 3, 2011. OSC ID: CPP20130223667002. <http://www.opensource.gov>.

67. Xinhua, “China Eyes Greater Market Share for its GPS Rival,” December 27, 2012. http://news.xinhuanet.com/english/china/2012-12/27/c_132066837.htm.

68. *Zhongguo Hangtian Bao* (China Aerospace News), “Pakistan to Become Fifth Asian Nation Employing Beidou Satellite Navigation System,” May 22, 2013. OSC ID: CHO2013071608611379. <http://www.opensource.gov>; Stephen Chen, “Thailand is Beidou Navigation Network’s First Overseas Client,” *South China Morning Post* (Hong Kong), April 4, 2013. <http://www.scmp.com/news/china/article/1206567/thailand-beidou-navigation-networks-first-overseas-client>.

69. *Want China Times*, “Pakistan Set to Adopt Beidou Navigation System: Report,” May 21, 2013. <http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20130521000095&cid=1101>.

70. Xinhua, “China’s Shenzhou-10 Mission Successful,” June 26, 2013. OSC ID: CPP20130626968125. <http://www.opensource.gov>; Rui Barbosa, “China’s Shenzhou-10 Successfully Docks with Tiangong-1,” *NASA Spaceflight.com*, June 13, 2013. <http://www.nasa.gov/spaceflight.com/2013/06/chinas-shenzhou-10-docks-tiangong-1/>.

71. Peter Shadbolt, "China Flexes its Space Muscles with Lesson in Zero Gravity," CNN, June 20, 2013. <http://www.cnn.com/2013/06/20/world/asia/china-space-lessons>.

72. CNTV, "China Announces Shenzhou-10 Mission 'Complete Success,'" June 26, 2013. OSC ID: CPP20130628010007. <http://www.opensource.gov>; Xinhua, "Xi Sees Off Shenzhou-10 Crew," June 11, 2013. http://news.xinhuanet.com/english/china/2013-06/11/c_132447946.htm.

73. *China Daily*, "China Expects to Complete Space Station by 2023," September 24, 2013. OSC ID: CHR2013092566656871. <http://www.opensource.gov>; Xinhua, "Shenzhou-10 Mission Marks Staged Success of China's Manned Space Programs: Vice Premier," June 26, 2013. http://news.xinhuanet.com/english/china/2013-06/26/c_132488037.htm; and *Renmin Ribao* (People's Daily), "3 Phases of China's Manned Space Program," June 17, 2013. english.peopledaily.com.cn/202936/8287313.html.

74. Information Office of the State Council (China), *China's Space Activities in 2011* (Beijing, China: December 29, 2011). http://www.china.org.cn/government/whitepaper/node_7145648.htm.

75. U.S.-China Economic and Security Review Commission, *Hearing on the Implications of China's Military and Civil Space Program*, written testimony of Scott Pace, May 11, 2011.

76. Zhao Zongqi, "An Important Aspect in Enhancing the Building of the Core Military Capability Is to, With Military Struggle Preparations as a Driving Force, Guarantee That the Armed Forces Will Fulfill Diversified Military Tasks in a Broader Sphere and Effectively Perform the Sacred Missions—Put the Building of the Strategic Delivery Capability to an Important Position," *Jiefangjun Bao* (PLA Daily), April 23, 2009. OSC ID: CPP20090429710001. <http://www.opensource.gov>; Nirav Patel, "Chinese Disaster Relief Operations: Identifying Critical Capability Gaps," *Joint Forces Quarterly* (1st Quarter, 2009) <http://www.hsdl.org/?view&did=32688>.

77. Zhao Huanxin, "Confidence Sky-High Over Jumbo Cargo Plane," *China Daily*, March 19, 2013. OSC ID: CPP20130319968029. <http://www.opensource.gov>.

78. Open Source Center, *Summary: PRC Expert Says Yun-20 Transport Makes Strategic Air Force Possible* (Washington, DC: January 27, 2013). OSC ID: CPP20130128787028. <http://www.opensource.gov>.

79. Open Source Center, *Summary: Guangdong Journal Views Strategic Card of Yun-20' Jumbo Air Freighter* (Washington, DC: January 31, 2013). OSC ID: CPP20130214695013. <http://www.opensource.gov>; Andrew Erikson and Gabe Collins, "The Y-20: China Aviation Milestone Means New Power Projection," *Wall Street Journal: China Real time Report*, January 28, 2013. <http://blogs.wsj.com/chinarealtime/2013/01/28/the-y-20-china-aviation-milestone-means-new-power-projection/>.

80. Zachary Keck, "Can China's New Strategic Bomber Reach Hawaii?" *Diplomat*, August 13, 2013. http://thediplomat.com/flashpoints-blog/2013/08/13/can-chinas-new-strategic-bomber-reach-hawaii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+the-diplomat+%28The+Diplomat+RSS%29; Noam Eshel, "Chinese Air Force Gets More H-6K Strategic Bombers," *Defense Update*, June 25, 2013. http://defense-update.com/20130625_h-6k-bombers-delivered-to-pla-air-force.html; and Chen Boyuan, "H-6K bombers delivered to PLA Air Force," *China.org.cn*, June 22, 2013. http://www.china.org.cn/china/2013-06/22/content_29197824.htm.

81. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: 2013), pp. 42, 81; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: 2011), p. 33.

82. Ian Easton, *The Assassin Under the Radar: China's DH-10 Cruise Missile Program* (Arlington, VA: The Project 2049 Institute, October 2009), pp. 1–6. http://project2049.net/documents/assassin_under_radar_china_cruise_missile.pdf.

83. Wendell Minnick, "China's Unmanned Aircraft Evolve from Figment to Reality," *Defense News*, November 26, 2012. <http://www.defensenews.com/article/20121126/DEFREG03/311260001/China-8217-s-Unmanned-Aircraft-Evolve-from-Figment-Reality?odyssey=tab/topnews/img/FRONTPAGE>.

84. Wendell Minnick, "Report: China's UAVs Could Challenge Western Dominance," *Defense News*, June 25, 2013. <http://www.defensenews.com/article/20130625/DEFREG03/306250021/Report-China-s-UAVs-Could-Challenge-Western-Dominance>.

85. Zhao Lei, "Foreign Buyers Eye Chinese Drones," *China Daily*, June 26, 2013. http://www.china.org.cn/business/2013-06/20/content_29174460.htm.

86. Brendan McGary, "China's Fighters, Drone Look Like U.S. Aircraft," *Defense Tech*, June 20, 2013. <http://defensetech.org/2013/06/20/chinas-fighters-drone-look-like-u-s-aircraft/>; David Cencotti, "Inside the Pterodactyl UAS: Sneak Preview of China's Predator Clone Mobile Ground Control Station," *Aviationist*, November 20, 2012.

<http://theaviationist.com/2012/11/20/pterodactyl/#.UkA6LIasiSo>; and Choi Chi-yuk, “Low-cost Chinese drone to be unveiled at Zhuhai Show,” *South China Morning Post* (Hong Kong), November 11, 2012. <http://www.scmp.com/news/china/article/1079637/low-cost-chinese-drone-be-unveiled-zhuhai-show>.

87. Edward Wong, “Hacking U.S. Secrets, China Pushes for Drones,” *New York Times*, September 20, 2013. http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html?_r=0; FireEye, “FireEye Advanced Threat Report—2H 2012,” pp. 14–18. <http://www2.fireeye.com/rs/fireeye/images/fireeye-advanced-threat-report-2h2012.pdf>.

88. FireEye, “FireEye Advanced Threat Report—2H 2012,” pp. 14–18. <http://www2.fireeye.com/rs/fireeye/images/fireeye-advanced-threat-report-2h2012.pdf>; Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units,” (Alexandria, VA: February 2013), p. 26. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

89. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: May 2013), p. 39; Senate Armed Services Committee, *Hearing on U.S. Pacific Command Posture*, written testimony of Admiral Samuel J. Locklear, 113th Cong., 1st sess., April 9, 2013.

90. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: May 2013), p. 39; Senate Armed Services Committee, *Hearing on U.S. Pacific Command Posture*, written testimony of Admiral Samuel J. Locklear, 113th Cong., 1st sess., April 9, 2013.

91. Daniel Ten Kate, “China Spurns Arbitration as U.S. Joins Japan on Sea Stance,” *Bloomberg*, June 2, 2013. <http://www.bloomberg.com/news/2013-06-02/china-spurns-sea-claim-arbitration-pushed-by-u-s-and-allies.html>; Rory Medcalf, “Maritime Game-Changer Revealed at Shangri-La Dialogue,” *Diplomat*, June 2, 2013. <http://the-diplomat.com/flashpoints-blog/2013/06/02/maritime-game-changer-revealed-at-shangri-la-dialogue/>.

92. United Nations Convention on the Law of the Sea, “Part 5: Exclusive Economic Zone.” http://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm; U.S.-China Economic and Security Review Commission, *2008 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2008), pp. 143–147.

93. Alan Wachman, “Playing by or playing with the rules of UNCLOS?” in Peter Dutton, ed. *Military Activities in the EEZ: A U.S.-China Dialogue on Security and International Law in the Maritime Commons* (Newport, RI: Naval War College, December 2010), p. 115.

94. U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), pp. 221, 239; Ronald O’Rourke, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress* (Washington, DC: Congressional Research Service, December 2012), pp. 4, 19.

95. Kathrin Hille, “Chinese navy begins US economic zone patrols,” *Financial Times* (London), June 2, 2013. <http://www.ft.com/intl/cms/s/0/02ce257e-cb4a-11e2-8ff3-00144feab7de.html#axzz2WDohYdhm>.

96. Ministry of Land and Resources (China), *Law of the People’s Republic of China on the Exclusive Economic Zone and Continental Shelf*. http://www.mlr.gov.cn/mlrenglish/laws/200710/t20071011_656313.htm.

97. Julian Ryall and Cary Huang, “China ramps up maritime strategy zone around US territory,” *South China Morning Post* (Hong Kong), June 4, 2013. <http://www.scmp.com/news/china/article/1252859/china-ramps-maritime-strategy>.

98. Daniel Ten Kate, “China Spurns Arbitration as U.S. Joins Japan on Sea Stance,” *Bloomberg*, June 2, 2013. <http://www.bloomberg.com/news/2013-06-02/china-spurns-sea-claim-arbitration-pushed-by-u-s-and-allies.html>; Rory Medcalf, “Maritime Game-Changer Revealed at Shangri-La Dialogue,” *Diplomat*, June 2, 2013. <http://the-diplomat.com/flashpoints-blog/2013/06/02/maritime-game-changer-revealed-at-shangri-la-dialogue/>.

99. Xinhua, “China to send peacekeeping force to Mali,” July 12, 2013; Ministry of National Defense (China), *Transcript of PRC National Defense Ministry’s News Conference on 27 June 2013* (Beijing, China: June 30, 2013). OSC ID: CPP20130627680001. <http://www.opensource.gov>; Ministry of Foreign Affairs (China), *Foreign Ministry Spokesperson’s Regular Press Conference on 27 June 2013* (Beijing, China: June 28, 2013). OSC ID: CPP20130628968145. <http://www.opensource.gov>; and Kathrin Hille, “China commits combat troops to Mali,” *Financial Times* (London), June 27, 2013. <http://www.ft.com/intl/cms/s/0/e46f3e42-defe-11e2-881f-00144feab7de.html#axzz2XoBd8ZiL>.

100. *China Defense Blog*, “Photos of the Day: The first PLA combat elements to Mali,” July 13, 2013. <http://china-defense.blogspot.com/2013/07/photos-of-day-first-pla-combat-elements.html>.

101. Ministry of National Defense (China), *Transcript of PRC National Defense Ministry’s News Conference on 27 June 2013* (Beijing, China: June 30, 2013). OSC ID: CPP20130627680001. <http://www.opensource.gov>; Ministry of Foreign Affairs (China), *Foreign Ministry Spokesperson’s Regular Press Conference on 27 June 2013* (Beijing, China: June 28, 2013). OSC ID: CPP20130628968145. <http://www.opensource.gov>; and Kathrin Hille, “China commits combat troops to Mali,” *Financial Times* (London), June 27, 2013. <http://www.ft.com/intl/cms/s/0/e46f3e42-defe-11e2-881f-00144feab7de.html#axzz2XoBd8ZtL>.

102. Xinhua, “China to Send Security Forces for Peacekeeping Mission in Mali,” June 27, 2013. OSC ID: CPP20130627968233. <http://www.opensource.gov>.

103. Daniel Hartnett, *China’s First Deployment of Combat Forces to a UN Peacekeeping Mission—South Sudan* (Washington, DC: U.S.-China Economic and Security Review Commission, March 13, 2012).

104. *Jiefangjun Bao* (PLA Daily), “First Chinese Peacekeeping Engineering Detachment to South Sudan Established,” January 5, 2012. OSC ID: CPP20120106702003. <http://www.opensource.gov>.

105. Zhao Shengnan and Pu Zhendong, “China, Russia Begin Live Fire Navy Drill,” *China Daily*, July 9, 2013. OSC ID: CHR2013070936047015. <http://www.opensource.gov>; *Jiefangjun Bao* (PLA Daily), “Six Highlights of China-Russia Maritime Joint Exercise,” July 5, 2013. OSC ID: CHO2013070821926494. <http://www.opensource.gov>.

106. *Jiefangjun Bao* (PLA Daily), “China-Russia Exercise ‘Joint Sea 2013’ in July,” July 10, 2013. OSC ID: CHO2013071018775963. <http://www.opensource.gov>; *Jiefangjun Bao* (PLA Daily), “China-Russia Naval Joint Exercise to be Normalized and Institutionalized,” July 11, 2013. OSC ID: CHL2013071132470531. <http://www.opensource.gov>.

107. CCTV-Xinwen, “PRC Expert Views Joint Antisubmarine, Air Defense Drills in China-Russia Naval Exercise,” July 10, 2013. OSC ID: CHO2013071018085524. <http://www.opensource.gov>.

108. Jeffrey Mankoff, “The Wary Chinese-Russian Partnership,” *New York Times*, July 11, 2013. http://www.nytimes.com/2013/07/12/opinion/global/the-wary-chinese-russian-partnership.html?_r=0.

109. Zachary Keck, “Russia Holds Massive Military Drill Aimed at China, Japan,” *Diplomat*, July 17, 2013. <http://thediplomat.com/flashpoints-blog/2013/07/17/russia-holds-massive-military-drill-aimed-at-china-japan/>.

110. Dean Cheng and Ariel Cohen, *How Washington Should Manage U.S.-Russia-China Relations* (Washington, DC: Heritage Foundation, September 12, 2013). http://www.heritage.org/research/reports/2013/09/how-washington-should-manage-us-russiachina-relations#_ftn16.

111. *Economist*, “India and China: Parsnips Unbattered,” May 25, 2013. <http://www.economist.com/news/asia/21578412-flowery-rhetoric-fails-hide-difficulties-bilateral-relationship-parasnips-unbattered>; Open Source Center, *Summary: India Protests PRC Troop ‘Intrusion’* (Washington, DC: April 23, 2013). OSC ID: FEA20130423030877. <http://www.opensource.gov>.

112. Ministry of Foreign Affairs (China), *Foreign Ministry Spokesperson Hua Chunying’s Regular Press Conference on April 25, 2013*, April 27, 2013. OSC ID: CPP20130427968070. <http://www.opensource.gov>.

113. Gardiner Harris, “India and China Vow to Cooperate on Border,” *New York Times*, May 20, 2013. http://www.nytimes.com/2013/05/21/world/asia/india-china-border-issues.html?_r=0.

114. Vivek Raghuvanshi, “India Sends Draft Border Cooperation Agreement to China,” *Defense News*, August 20, 2013. <http://www.defensenews.com/article/20130820/DEFREG03/308200026/India-Sends-Draft-Border-Cooperation-Agreement-China>.

115. Ely Ratner and Alexander Sullivan, “The Most Dangerous Border in the World: Why is China picking a fight with India?” *Foreign Policy*, May 4, 2013. http://www.foreignpolicy.com/articles/2013/05/03/china_india_most_dangerous_border?page=0,0.

116. U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), p. 11.

117. Josh Rogin, “Former top U.S. official: China getting fed up with North Korea,” *Foreign Policy*, April 5, 2013. http://thecable.foreignpolicy.com/posts/2013/04/05/former_top_us_official_china_getting_fed_up_with_north_korea.

118. William Wan, "Chinese President Xi Jinping expresses concern over North Korea's rhetoric," *Washington Post*, April 7, 2013. http://articles.washingtonpost.com/2013-04-07/world/38354043_1_south-china-sea-schumer-united-nations.

119. Jane Perlez, "China Bans Items for Export to North Korea, Fearing Their Use in Weapons," *New York Times*, September 24, 2013. <http://www.nytimes.com/2013/09/25/world/asia/china-bans-certain-north-korean-exports-for-fear-of-weapons-use.html>.

120. Roger Cavazos, Peter Hayes, and David von Hippel, "Technical Bulletin #59 on Prohibition of Dual Use Exports to North Korea," Nautilus Institute for Security and Sustainability, September 26, 2013. <http://nautilus.org/napsnet/napsnet-special-reports/technical-bulletin-59-on-prohibition-of-dual-use-exports-to-north-korea/#axzz2h4TEY8ZL>.

121. United Nations Security Council, "Security Council Strengthens Sanctions on Democratic People's Republic of Korea, In Response to 12 February Nuclear Test," March 7, 2013. <http://www.un.org/News/Press/docs/2013/sc10934.doc.htm>.

122. Stephanie Kleine-Ahlbrandt, "China's North Korea Policy: Backtracking from Sunnylands?" 38North.org, July 2, 2013. <http://38north.org/2013/07/skahlbrandt070213/>.

123. Stephanie Kleine-Ahlbrandt, "China's North Korea Policy: Backtracking from Sunnylands?" 38North.org, July 2, 2013. <http://38north.org/2013/07/skahlbrandt070213/>.

124. Joel Wuthnow, "How China Reads North Korea," *National Interest*, September 8, 2013. <http://nationalinterest.org/commentary/how-china-reads-north-korea-9009>.

125. Michael S. Chase, "China's Search for a 'New Type of Great Power Relationship,'" *China Brief* 12:27 (Washington, DC: Jamestown Foundation, September 7, 2012), p. 14. http://www.jamestown.org/uploads/media/cb_09_04.pdf.

126. Xinhua, "China, U.S. agree to build new type of relations," June 8, 2013. http://news.xinhuanet.com/english/china/2013-06/08/c_132442379.htm; Jeremy Page and Colleen McCain Nelson, "U.S.-China Summit Reveals Beijing's Drive," *Wall Street Journal*, June 2, 2013. <http://online.wsj.com/article/SB10001424127887324423904578521161140840702.html>; and Jamil Anderlini, "Global Insight: China's 'great power' call to the US could stir friction," *Financial Times* (London), June 4, 2013. <http://www.ft.com/intl/cms/s/0/80f4168a-ccca-11e2-9cf7-00144feab7de.html#axzz2WfPEh45n>.

127. Zhao Xiaozhuo, "The Building of a New-Type Military Relationship Between China and the United States Is Facing a Historic Opportunity," *Jiefangjun Bao* (PLA Daily), June 14, 2013. OSC ID: CPP20130614787003. <http://www.opensource.gov>.

128. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: May 2013), pp. 69–71.

129. Karen Parrish, "U.S.-China Military Ties Growing, Pacom Commander Says," U.S. Armed Forces Press Service, July 11, 2013. <http://www.defense.gov/news/newsarticle.aspx?id=120440>.

130. Karen Parrish, "Leaving Asia, Dempsey Discusses Combined Defense, China Engagement," U.S. Armed Forces Press Service, April 27, 2013. <http://www.defense.gov/news/newsarticle.aspx?id=119894>.

131. N. Ross Taylor, "USS Shiloh Sailors Visit Zhanjiang, China," U.S. Navy News Service, May 30, 2013. http://www.navy.mil/submit/display.asp?story_id=74477.

132. Matthew White, "USS Fitzgerald Arrives in Qingdao, China," U.S. Department of Navy, April 20, 2009. http://www.navy.mil/submit/display.asp?story_id=44493.

133. *Renmin Ribao* (People's Daily), "Wu Shengli meets with U.S. Pacific Fleet commander," May 30, 2013. english.peopledaily.com.cn/90786/8263856.html; Xinhua, "China, US vow further naval cooperation," May 28, 2013. http://news.xinhuanet.com/english/china/2013-05/28/c_132414858.htm.

134. Grace Jean, "USN Cruiser, US Pacific Fleet Commander Stop in China for Scheduled Port Visit," *IHS Jane's Navy International*, May 30, 2013. <http://www.janes.com/article/12842/usn-cruiser-us-pacific-fleet-commander-stop-in-china-for-scheduled-port-visit>.

135. U.S. Chief of Naval Operations, *CNO Wraps up Weeklong Visit with PLA Navy* (Washington, DC: August 16, 2013). http://www.navy.mil/search/print.asp?story_id=76608&VIRIN=&imagetype=0&page=0.

136. Cynthia Clark, "Chinese Navy Ships Visit Hawaii," U.S. Navy News Service, September 7, 2013. http://www.navy.mil/submit/display.asp?story_id=76402.

137. Associated Press, "Chinese ships head for search exercises with US Navy as Beijing ramps up military diplomacy," August 20, 2013. http://www.washingtonpost.com/world/asia_pacific/chinese-ships-depart-for-rare-drills-with-us-navy-as-beijing-ramps-up-military-diplomacy/2013/08/20/4499d6c0-0a05-11e3-89fe-abb4a5067014_story.html; U.S. Department of Defense, *Department of Defense Press Briefing with Secretary Hagel and Gen. Chang from the Pentagon* (Washington, DC: August 19, 2013). <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5289>.

138. Donna Miles, "U.S., Chinese Navies Exercise Counterpiracy in Gulf of Aden," U.S. American Forces Press Service, August 26, 2013. <http://www.defense.gov/news/newsarticle.aspx?id=120675>.

139. U.S. Department of Defense, *Department of Defense Press Briefing with Secretary Hagel and Gen. Chang from the Pentagon* (Washington, DC: August 19, 2013). <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5289>.

140. U.S. Chief of Naval Operations, *CNO Wraps up Weeklong Visit with PLA Navy* (Washington, DC: August 16, 2013). http://www.navy.mil/search/print.asp?story_id=76608&VIRIN=&imagetype=0&page=0.

141. Shirley Kan, *U.S.-China Military Contacts: Issues for Congress* (Washington, DC: Congressional Research Service, July 25, 2013).

142. Karen Parrish, "U.S.-China Military Ties Growing, PACOM Commander Says," U.S. American Forces Press Service, July 11, 2013. <http://www.defense.gov/news/newsarticle.aspx?id=120440>.

143. James Hardy, "Back to the Future: The U.S. Navy Returns to The Philippines," *Diplomat*, October 16, 2012. <http://thediplomat.com/2012/10/16/just-like-old-times-us-navy-returns-to-philippines/?all=true>.

SECTION 2: CHINA'S CYBER ACTIVITIES

Introduction

Since the Commission's *2012 Annual Report to Congress*, strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States. This section—based on discussions with cybersecurity experts and U.S. Department of Defense (DoD) officials and independent research*—provides an overview of this evidence, examines developments in Chinese cyber policy, and explores potential U.S. actions and policies to deter and mitigate future Chinese cyber theft and improve U.S. cyber policy development and implementation.†

Mounting Evidence of the Chinese Government's Active Role in Cyber Espionage

Detailed Technical Information Released on Chinese Cyber Activities

In February 2013, Mandiant, a private U.S. cybersecurity firm, published a report providing detailed technical information regarding the activities of a cyber threat group, which Mandiant refers to as Advanced Persistent Threat 1. According to the report, the group likely is the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's Third Department, also known as Unit 61398. Mandiant assesses Unit 61398 since 2006 has penetrated the networks of at least 141 organizations, including companies, international organizations, and foreign governments. These organizations are either located or have headquarters in 15 countries and represent 20 sectors, from information technology to financial services. Four of these sectors are among the seven strategic emerging industries the Chinese government prioritized for development in its 12th Five-Year Plan (2011 to 2015). 81 percent of the targeted organizations were either located in the United States or had U.S.-based headquarters. Through these intrusions, the group gained access to "broad categories of intellectual prop-

*In 2013 the Commission held a roundtable on U.S.-China cybersecurity issues on July 11 and sponsored a report on the economic and security implications of cloud computing development in China, which the Commission published on September 5. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013). http://origin.www.uscc.gov/sites/default/files/Research/Red%20Cloud%20Rising_Cloud%20Computing%20in%20China.pdf.

†For discussion of China's cyber strategy and actors, see U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), pp. 147–151; Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012). http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

erty, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and e-mails and contact lists from victim organizations' leadership."¹

In its report, Mandiant states Unit 61398 is responsible for conducting computer network operations,* specifically the gathering of strategic and economic intelligence on targets in the United States and Canada, as well as targeting organizations whose primary language is English in other countries.² Aside from Unit 61398, the Third Department has another 11 operational bureaus, three research institutes, four operations centers, and 16 technical reconnaissance bureaus.[†]³ Not all of these organizations are directing their actions against the United States, and there are no public reports available about their role in China's cyber espionage campaign.⁴

According to the *Wall Street Journal*, on the same day Mandiant published its report, the U.S. Department of Homeland Security and the U.S. Federal Bureau of Investigation shared hundreds of Internet Protocol (IP) addresses used by Unit 61398 with U.S. Internet service providers to help them defend their customers against cyber intrusions. Mandiant gave the U.S. government advance notice of the release of its report on Unit 61398; this may have been a factor in the timing of the government's sharing of the IP addresses.⁵

In April 2013, the Verizon RISK Team, a cybersecurity unit within private U.S. telecommunications company Verizon, published its annual *Data Breach Investigations Report*.⁶ The report presents analysis of 621 cases of "confirmed data disclosure," which Verizon defines as "any event resulting in confirmed compromise (unauthorized viewing or accessing) of any non-public information," that occurred in 2012. Eighteen governmental and private organizations from the United States, Europe, Malaysia, and Australia provided the information about these cases. Verizon categorized 19 percent of the intrusions as espionage carried out by "state-affiliated actors." It identified 96 percent of the intrusions conducted by state-affiliated actors as originating in China.⁷

Chinese Cyber Espionage against U.S. Critical Infrastructure

In July 2013, a threat researcher at Trend Micro, a private Japanese cybersecurity firm, claimed he had detected a Chinese cyber intrusion, commencing in December 2012, of a honeypot.[‡]

*Computer network operations are "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations." Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012), p. 115. http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

† Technical reconnaissance bureaus are administratively subordinate to the PLA General Staff Department's Third Department but are attached to the PLA's service arms and provide direct support to operational units through signals intelligence and computer network operations.

‡ A honeypot is part of a honeynet, which is a fake or diversionary computer network designed to draw in an adversary in order to identify the adversary or give the adversary false information. Honeynets can provide intelligence regarding adversaries' "tools, tactics, and motives." The

Chinese Cyber Espionage against U.S. Critical Infrastructure—Continued

He created the honeypot to resemble the industrial control system of a water plant in the United States. The researcher attributed the intrusion to Unit 61398, based on forensic analysis.⁸ If true, this suggests Unit 61398 is collecting intelligence on critical infrastructure in addition to other targets. Such activities are consistent with PLA doctrine, which explains that one function of wartime computer network operations is to “disrupt and damage the networks of [an adversary’s] infrastructure facilities, such as power systems, telecommunications systems, and educational systems.”⁹ Some PLA strategists also have suggested China should develop the capability to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.¹⁰

U.S. Department of Defense for the First Time Attributes Cyber Espionage to China

In May 2013, DoD for the first time directly accused the Chinese government and military of cyber espionage against U.S. networks. DoD’s 2013 *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China* states: “In 2012, numerous computer systems around the world, including those owned by the U.S. government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military.” The report then states, “China is using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs.”¹¹

U.S. Secretary of Defense Chuck Hagel said addressing Chinese cyber espionage primarily requires dialogue between the U.S. and Chinese governments behind closed doors, but he added, “It has to be public as well.”¹² Publicly attributing cyber intrusions to the Chinese government and military in the DoD report is a significant step for the U.S. government. Previous DoD documents and statements had acknowledged cyber espionage “emanated” or “originated” from China but stopped short of attributing those operations to the Chinese government and military. For example, DoD’s 2012 report to Congress stated: “Computer networks and systems around the world continued to be targets of intrusions and data theft, many of which originated within China.”¹³ In a press briefing following the release of the 2012 report, then acting Deputy Assistant Secretary of Defense for East Asia David Helvey said, “We have concerns about a number of computer network operations and activities that appear to originate from China that affect DoD networks.” When asked whether he was referring to the Chinese government, he said, “I didn’t specify the attribution.”¹⁴

Honeynet Project, “Short Video Explaining Honeypots.” <http://old.honeynet.org/misc/files/HoneynetWeb.mov>.

Beijing Issues Routine Denials of the Allegations by Mandiant and DoD

When confronted with public accusations from the United States about its cyber espionage, Beijing attempted to refute the evidence, in part, by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. The Chinese government's statements were similar to its responses to previous foreign allegations of cyber espionage.¹⁵

In a press conference on the day after Mandiant released its report, a spokesperson for China's Ministry of Foreign Affairs said, "Groundless speculation and accusations regarding hacker attacks, for various purposes, is both unprofessional and irresponsible and it is not helpful for solving the problem." He also emphasized cyber attacks are a serious problem for China.¹⁶ In a press conference the next day, a spokesperson for China's Ministry of National Defense denied that the PLA supports hacking. He argued Mandiant's allegations are without merit, because, among other reasons, hackers frequently use third-party IP addresses to conduct cyber attacks.¹⁷

In response to the allegations regarding China's cyber espionage activities in DoD's 2013 report to Congress, a Ministry of Foreign Affairs spokesperson said China is "strongly against any form of hacking activities" and called the charges "baseless."¹⁸

Evidence of a Cyber Campaign against U.S. Press

There is growing evidence the Chinese government is conducting a cyber espionage campaign against U.S. media organizations. China likely seeks to use information acquired through these intrusions to (1) shape U.S. press coverage of China by intimidating U.S. journalists' sources in China, and (2) gain warning about negative media coverage of China before it is published.¹⁹

- In January 2013, the *New York Times* reported Chinese cyber actors had gained access to its computer network in September 2012 and had conducted activities inside the network for the next four months. The intrusions appeared to focus on the e-mail account of a reporter investigating the assets of family members of outgoing Chinese Premier Wen Jiabao. The *New York Times* hired Mandiant to investigate the intrusion, which Mandiant attributed to a China-based cyber threat group it refers to as Advanced Persistent Threat 12. The *New York Times* reported, "The attacks started from the same university computers used by the PLA to attack United States military contractors in the past."²⁰
- The *New York Times* also reported Chinese cyber actors conducted an intrusion into computers at Bloomberg News in 2012 following Bloomberg's investigation of the assets of then Chinese Vice President Xi Jinping's relatives.²¹
- Following the *New York Times*' revelations, the *Wall Street Journal* and the *Washington Post* reported their networks also had been penetrated by hackers, with evidence in both cases implicating cyber actors based in China.²² In the *Wall Street*

Journal intrusion, the hackers targeted personnel reporting on China.²³

New Information Emerges about 2009 Intrusion into Google's Network

In May 2013, the *Washington Post* reported Chinese cyber actors in 2009 infiltrated a Google database containing information regarding Foreign Intelligence Surveillance Court orders Google had received.* The hackers seemed to be searching for names of Chinese intelligence operatives whom the U.S. government might be monitoring. Regarding this intrusion, a former U.S. government official said that were the Chinese government to become aware that its operatives were being monitored, it could “take steps to destroy information, get people out of the country,” and perhaps intentionally transmit incorrect information to the U.S. government.²⁴ A former U.S. Department of Justice (DoJ) official said data breaches such as this one show “the overall security and effectiveness of lawful interception and undercover operations is dependent in large part on security standards in the private sector,” which “clearly need strengthening.”²⁵

Defense Science Board Points to Widespread Hacking of U.S. Defense Designs

The Defense Science Board † warns in *Resilient Military Systems and the Advanced Cyber Threat*, an unclassified report published in October 2012, “The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War.” The Defense Science Board then assesses DoD “is not prepared to defend against this threat.”²⁶ In May 2013, the *Washington Post* published an article describing a classified version of the report, which lists more than 24 U.S. weapon system designs the board determined were accessed by cyber intruders. The *Washington Post* reported, “Senior military and industry officials with knowledge of the breaches said the vast majority were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies.” The list includes the Patriot Advanced Capability 3 air defense system, the Terminal High Altitude Area Defense system, the Aegis ballistic missile defense system, the F/A-18 fighter aircraft, the V-22 Osprey multirole combat aircraft, the Black Hawk helicopter, the Littoral Combat Ship, and the F-35 Joint Strike Fighter.²⁷

*The intruders also reportedly accessed Google's source code. Source code is the set of instructions that compose computer software programs. In addition, they attempted to access the e-mail accounts of Chinese human rights activists. This intrusion was part of a broader campaign targeting over 30 companies that U.S. cybersecurity company McAfee called “Operation Aurora.” Ellen Nakashima, “Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say,” *Washington Post*, May 20, 2013. http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi; Andrew Jacobs and Miguel Helft, “Google, Citing Attack, Threatens to Exit China,” *New York Times*, January 13, 2010. <http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all&r=0>; and Kim Zetter, “Google Hack Attack Was Ultra Sophisticated, New Details Show,” *Wired*, January 14, 2010. <http://www.wired.com/threatlevel/2010/01/operation-aurora/>.

† According to its charter, the Defense Science Board submits “independent advice and recommendations on science, technology, manufacturing, acquisition process, and other matters of special interest to the DoD” to the Secretary of Defense and other senior defense officials. Defense Science Board, “Charter.” <http://www.acq.osd.mil/dsb/charter.htm>.

Update on U.S. Department of Justice Indictment of Chinese Company

In another high-profile example of a Chinese company allegedly targeting a U.S. company's intellectual property through cyber espionage, the DoJ in June 2013 filed charges against Sinovel Wind Group, a Chinese energy firm, alleging Sinovel stole intellectual property from Massachusetts-based company American Superconductor (AMSC). DoJ charged Sinovel, the deputy director of Sinovel's research and development department, a technology manager at Sinovel, and a former employee of a subsidiary of AMSC with theft of trade secrets and related charges.²⁸

AMSC and Sinovel entered into a business relationship in 2005, with AMSC selling software, components, and electrical systems to Sinovel for use in its wind turbines. In the following years, Sinovel became AMSC's largest client. However, the Chinese firm in 2011 stopped paying for products that had arrived in China and cancelled existing orders after allegedly stealing source code from AMSC to reproduce AMSC's software.²⁹ Media reporting alleges Dejan Karabasevic, who was working as an engineer for AMSC Wintec GmbH in Austria at the time, remotely extracted the source code from a computer in Wisconsin and delivered it to Sinovel by e-mail.³⁰ According to the company's chief executive officer, without sales to Sinovel, AMSC's revenue declined dramatically, and 50 percent of its 900 employees lost their jobs.³¹ In early 2012, the U.S. Federal Bureau of Investigation found software alleged to have been illegally copied from AMSC's software in a wind turbine the Massachusetts Water Resources Authority had purchased from Sinovel. This was a critical factor leading to Sinovel's indictment.³² AMSC has sought compensation from Sinovel through lawsuits in China, an effort that is ongoing and has resulted in legal fees for AMSC exceeding \$6 million.³³

Chinese Cyber Policy Developments

United States and China Establish Cyber Working Group

In April 2013, U.S. Secretary of State John Kerry announced the U.S. and Chinese governments would establish a working group to discuss cybersecurity.³⁴ The Cyber Working Group convened for the first time in July immediately preceding the latest meeting of the U.S.-China Strategic and Economic Dialogue (S&ED). Christopher Painter, the U.S. Department of State's Coordinator for Cyber Issues, and Dai Bing, an official from China's Ministry of Foreign Affairs, were the senior representatives for their respective countries at the meeting.³⁵ At the conclusion of the S&ED, the two sides announced they had "decided to take practical measures to enhance dialogue on international norms and principles in order to guide action in cyber space and to strengthen CERT to CERT (Computer Emergency Response Team)* coordination and cooperation."³⁶ James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies

*A CERT is an organization that is devoted to preventing and resolving cybersecurity problems and provides information regarding cyber threats and vulnerabilities to government agencies, companies, and other organizations. For an example of a CERT, see US-CERT, "About Us" (Washington, DC: U.S. Department of Homeland Security). <http://www.us-cert.gov/about-us>.

(CSIS), testified to the House Foreign Affairs Committee's Subcommittee on Asia and the Pacific that the July S&ED and Cyber Working Group meetings "are an important step that, if it succeeds, will make the situation in Asia more stable." He added, "We are looking at a long effort and the S&ED process will need to be sustained and reinforced."³⁷

China Shifts on International Law and Cyberspace

In what appears to be a break with the past, China in June 2013 agreed in a United Nations (UN) report that international law, which includes the law of armed conflict,* extends to cyberspace. The report states, "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible [information and communication technology] environment."³⁸ In addition, China agreed that "states must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of [information and communication technologies]."³⁹ This statement is based on the contents of the UN's *Articles on Responsibility of States for Internationally Wrongful Acts*, also known as the law of state responsibility.⁴⁰ The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which includes China, the United States, Russia, and 12 other countries, agreed on the report's contents when the group convened in New York.⁴¹

James Mulvenon, vice president of Defense Group Inc.'s Intelligence Division, at the roundtable on U.S.-China cybersecurity issues held by the Commission on July 11, said, "The Chinese made a dramatic reversal on their view about how the laws of armed conflict did not apply to the cyber dimension, which was a showstopper for DoD about [the department] being involved in any confidence building measures [with China]."⁴² While the Chinese government does not appear to have publicly asserted its stance on the applicability of the law of armed conflict and the law of state responsibility to cyberspace prior to the UN report, U.S. experts and media reports indicate that in the past Beijing has not agreed that these laws apply to activities in cyberspace.⁴³

Impact of Snowden Leaks on U.S. Efforts to Stop Chinese Cyber Espionage

In June 2013, Edward Snowden, a former contractor for the U.S. National Security Agency (NSA) alleged NSA has conducted cyber operations against hundreds of Hong Kong and mainland Chinese targets.⁴⁴ Addressing Mr. Snowden's allegations, a

*The law of armed conflict, which is also known as international humanitarian law, includes principles such as distinction between military and civilian targets, proportionality, military necessity, and limitation. International Committee of the Red Cross, "The Law of Armed Conflict: Basic Knowledge," June 2002, pp. 12–14. http://www.icrc.org/eng/assets/files/other/law1_final.pdf.

Impact of Snowden Leaks on U.S. Efforts to Stop Chinese Cyber Espionage—Continued

spokesperson for China's Ministry of National Defense said, "To, on the one hand, abuse one's advantages in information technology for selfish ends, while on the other hand, making baseless accusations against other countries, shows double standards that will be of no help for peace and security in cyberspace."⁴⁵ Despite the Obama Administration's efforts to distinguish what it calls "cyber-enabled economic espionage" or "cyber-enabled theft of trade secrets" from government-to-government espionage,⁴⁶ some observers expect Mr. Snowden's allegations to set back U.S. efforts on U.S.-China cybersecurity issues by at least six months. Dr. Mulvenon said, "I don't really think we're going to make a lot of progress for a while. . . . I would say it's probably going to delay progress six to twelve months."⁴⁷ However, an official at the U.S. embassy in Beijing told the Commission Mr. Snowden's allegations had not affected private discussions with the Chinese government on cyber theft of intellectual property.

Developments Related to Chinese Information Technology Companies

An October 2012 report by the U.S. House Permanent Select Committee on Intelligence (HPSCI) characterized China's two largest telecommunication equipment companies, Huawei and ZTE, as a risk to U.S. national security because they could facilitate intelligence collection by the Chinese government. The report advised U.S. companies against using products or services provided by Huawei and ZTE.^{*48} During an interview with the *Australian Financial Review* in July 2013, former director of the Central Intelligence Agency and NSA, General Michael Hayden (Retd.), confirmed and augmented the HPSCI's findings regarding Huawei. When asked to verify whether he believed "it is reasonable to assume that hard evidence exists that Huawei has engaged in espionage on behalf of the Chinese state," General Hayden said, "Yes, that's right." He then added, "At a minimum, Huawei would have shared with the Chinese state intimate and extensive knowledge of the foreign telecommunications systems it is involved with. I think that goes without saying."⁴⁹

Huawei and ZTE continue to issue public assurances that they do not pose a security threat.⁵⁰ For example, Huawei's president Ren Zhengfei said during his first interview with a media organization in May 2013 that his company would not assist the Chinese government with collecting foreign intelligence if asked.⁵¹

Despite widespread concerns about the national security risks posed by Huawei and ZTE, Bloomberg reported in August 2013 that the U.S. General Services Administration (GSA) authorized U.S. government agencies to procure a videoconferencing system produced by ZTE and Prescient, a division within U.S. company CyberPoint International LLC, in November 2012. According to an

*For more details on the HPSCI report, see U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), p. 164.

executive at CyberPoint, Prescient produced hardware and software to enhance the security of the system, which was originally made by ZTE. He said, due to these alterations, it now was a “Made-in-America product.”⁵² However, in September 2013, U.S. Customs and Border Protection concluded the system should still be considered a Chinese product, because “the Chinese-origin Video Board and the Filter Board impart the essential character to the video teleconferencing server.”⁵³ GSA subsequently took the system off the list of products agencies can buy. Even before the decision, no U.S. agencies had purchased this product.⁵⁴

In a meeting in May 2013, Commissioners and DoD officials discussed DoD’s interpretation of U.S. law regarding procurement sources. DoD officials indicated a stricter procurement evaluation standard that includes sourcing concerns could be applied only to items on the United States Munitions List. Items outside this list are judged by a different standard, which some officials believe might preclude concerns about the origin of products. For example, items procured for C4ISR* maintenance facilities are not subject to stricter scrutiny. Commissioners raised concerns that this interpretation of the law was limiting the department’s ability to address potential risks arising from certain procurement sources. Commissioners urged DoD to expand the purview of the stricter standard to items beyond the munitions list.

DoD is currently moving in this direction. Section 806 of the National Defense Authorization Act (NDAA) for Fiscal Year 2011 is intended to address the problem, but it has yet to be fully implemented. Section 806 authorizes the Secretary of Defense and the secretaries of the Army, Navy, and Air Force to reject procurement sources for information technology on grounds of protecting supply chain security if they receive a recommendation to do so from DoD.⁵⁵ According to a DoD Congressional liaison, as of May, “DoD has proceeded to implement NDAA Section 806, beginning with a number of table-top exercises involving department procurement, legal, acquisition, engineering, and intelligence experts to expose any underlying issues with 806 implementation.”⁵⁶ In addition, DoD wrote the Defense Federal Acquisition Regulation Supplement Rule implementing Section 806 and, as of May, the rule was in the process of interagency coordination.⁵⁷ These changes to DoD procurement ultimately may provide officials with the flexibility they need to protect all DoD systems. However, progress has been slow and the problem the Commissioners highlighted will remain until the new policy is implemented, potentially posing a threat to national security.

Security Implications of Cloud Computing in China

“Cloud computing, often referred to as simply ‘the cloud,’ is the delivery of on-demand computing resources—everything from applications to data centers—over the Internet and on a pay-for-use basis,” according to IBM.⁵⁸ In *Red Cloud Rising: Cloud Computing in China*, a report for the Commission published in 2013, Defense

* C4ISR refers to command, control, communications, computers, intelligence, surveillance, and reconnaissance.

Group Inc. (DGI) describes several potential cybersecurity concerns related to China and cloud computing, including the following:

- Microsoft licensed 21Vianet, a Chinese data center services company, to provide Office 365 and Windows Azure, two cloud computing products, to customers in China. Microsoft currently plans to link 21Vianet's data centers in China to Microsoft's data centers in other parts of Asia, Europe, and North America. As a part of this plan, Windows Azure users outside China could choose to store their data in data centers in China, and Azure users in China could store their data in other countries. Domestic Chinese law authorizes the government to "inspect the electronic communication instruments and appliances and other similar equipment and installations" of organizations operating in China. If the Chinese government accesses 21Vianet's data centers, it might then potentially connect to foreign data centers through the network Microsoft is planning. DGI states, "This risk can be mitigated by designing the network with appropriate data segregation and limits on network administrator privileges."⁵⁹
- China's Ministry of State Security (MSS), the country's main foreign intelligence collection agency, is closely connected with the Chongqing Special Cloud Computing Zone. In addition to being one of the central government agencies to authorize the establishment of the zone, the MSS has stated it is giving the zone "leading guidance and corresponding requirements."⁶⁰ The agency's connection to this cloud computing zone represents a potential espionage threat to foreign companies that might use cloud computing services provided from the zone or base operations there.⁶¹
- Since Chinese domain registrars and Internet service providers typically are not vigilant about users employing their services to carry out nefarious activities against computers outside China, DGI writes, "One can speculate that malicious use of Chinese cloud services may eventually take place at a higher rate than the cloud computing industry's global norm."⁶²
- Given the widely acknowledged security weaknesses in networking hardware developed by Chinese companies and the shift toward use of this equipment in Chinese cloud infrastructure, "it logically follows that use of this equipment may constitute an additional vulnerability in some Chinese cloud infrastructure, beyond the standard 'baseline' level of vulnerability."⁶³

In addition, cloud computing could improve the PLA's C4ISR capabilities. DGI writes that cloud computing "could enable more effective and flexible development and deployment of military equipment, while at the same time improving the survivability of the PLA's information systems by endowing them with greater redundancy (allowing a system's capabilities to survive the disabling or destruction of any individual node)."⁶⁴

Deterring Chinese Cyber Theft against U.S. Companies

There are no indications the public exposure of Chinese cyber espionage in technical detail throughout 2013 has led China to change its attitude toward the use of cyber espionage to steal intellectual property and proprietary information. Mandiant's revelations merely led Unit 61398 to make changes to its cyber "tools and infrastructure," causing future intrusions to be harder to detect and attribute.⁶⁵ Richard Bejtlich, chief security officer at Mandiant, said Unit 61398 decreased its activity for about one month following the publishing of Mandiant's report in February.⁶⁶ Former and current U.S. officials said the U.S. government's sharing of IP addresses with Internet service providers contributed to this reduction in activity.⁶⁷ However, Mr. Bejtlich said Unit 61398 remains active but at lower levels compared to the period before Mandiant's report was released.⁶⁸

It is clear naming and attempting to shame will not be sufficient to deter entities in China from engaging in cyber espionage against U.S. companies. Mitigating the problem will require a long-term and multifaceted approach that centers on changing China's cost-benefit calculus.⁶⁹ Congress, the Obama Administration, and outside experts are discussing a number of potential U.S. actions and policies, including the following:

Link Chinese economic cyber espionage to trade restrictions. An example of such a measure is the *Deter Cyber Theft Act* (S. 884), a bipartisan bill introduced in the Senate in May 2013. The bill requires the U.S. intelligence community to identify goods it assesses to have been "manufactured or otherwise produced using technologies or proprietary information" that was "developed by United States persons" and acquired through cyber espionage. It calls on the President to block the import of these goods if the President deems it necessary for safeguarding intellectual property rights or the DoD supply chain.⁷⁰

Prohibit Chinese firms using stolen U.S. intellectual property from accessing U.S. banks. In May 2013, the Commission on the Theft of American Intellectual Property (hereafter "the IP Commission"),* released a report that examines the pilfering of U.S. intellectual property and presents policy recommendations to address the problem. The IP Commission recommends the U.S. government "deny the use of the American banking system to foreign companies that repeatedly benefit from the misappropriation of American intellectual property."⁷¹ Roy Kamphausen, senior advisor for political and security affairs at the National Bureau of Asian Research and the deputy executive director for the IP Commission, explained at the Commission's roundtable the U.S. government could determine whether or not a foreign company should be sanctioned based on a combination of information from commercial or government sources, and well-defined bench-

*The IP Commission was co-chaired by Dennis Blair, former U.S. director of national intelligence, and Jon Huntsman, former U.S. ambassador to China.

**Deterring Chinese Cyber Theft against U.S. Companies—
Continued**

marks, such as the results of legal cases in the past involving the company.⁷²

Ban U.S. travel for Chinese organizations that are involved with cyber espionage. Dr. Mulvenon suggested to the Commission the United States needs “to create a constituency of people in China who want to succeed but are being harmed by government cyber espionage efforts that they had nothing to do with.” He believes placing Chinese companies and universities involved with cyber espionage on a list of entities that are barred from entry into the United States would help to build this constituency. However, Dr. Mulvenon warned this policy would have to be implemented carefully and deliberately, because sanctioning Chinese companies that are connected to foreign multinational companies “would be self-defeating in some cases.”⁷³ For example, if a U.S. company has a partnership with a Chinese company, such measures might hinder the U.S. company’s ability to do business with its Chinese partner.

*Use counterintelligence techniques, such as deliberately providing incorrect information to cyber spies to “poison the well.”*⁷⁴ Dr. Mulvenon explained to the Commission this could lead the Chinese government “to spend more and more resources actually figuring out whether things are true or not.” He argued, “The more problems they have in that system will lead them to begin to accelerate the trends toward centralization of authority and decision-making, and . . . I think the goal of our policy should be to make it as difficult to get a computer network exploit operation approved in the Chinese system as it is currently in our system.”^{*75} However, David Merkel, Mandiant’s chief technology officer, doubts the effectiveness of this tactic. He said, “Those kinds of techniques can be effective in highly-targeted ways, used by specialists to get some particular result like learning more information about an adversary . . . but as some kind of broad-based defense or mechanism to change the economics of stealing digital information, I just don’t see it.”⁷⁶ Mr. Merkel explained, “When I go take a look at a large organization and the challenges it has managing its own legitimate information, and then you talk about managing legitimate disinformation and being able to tell one from the other and being able to make decisions based on what happens with it seems pretty far fetched.”⁷⁷

Encourage the U.S. government, military, and cleared defense contractors to implement measures to reduce the effectiveness of Chinese cyber operations and increase the risk of conducting such operations for Chinese organizations. For example, the IP Commission recommends measures such as “meta-tagging, water-

*Dr. Mulvenon said that in China there is a “bottom up, grassroots, entrepreneurial sort of cyber espionage framework.” He described U.S. cyber espionage as “top down . . . and controlled,” and involving a great deal of oversight. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

**Deterring Chinese Cyber Theft against U.S. Companies—
Continued**

marking, and beaconing,”⁷⁸ because they can help identify sensitive information and code a digital signature within a file to better detect intrusion and removal.⁷⁹ These tags also might be used as evidence in criminal, civil, or trade proceedings to prove data was stolen.

Clarify the legal rights of companies, and the types of action that are prohibited, regarding finding and recovering intellectual property that is stolen through cyber intrusions. Mr. Kamphausen said U.S. companies “need the right tools that afford them the protections, legal and otherwise, so that they can do what’s in their own interest.”⁸⁰

Pass legislation permitting U.S. companies to conduct offensive cyber operations in retaliation against intrusions into their networks. Such operations could range from “actively retrieving stolen information” to “physically disabling or destroying the hacker’s own computer or network.” The IP Commission explores this option in its report but ultimately does not endorse it at the current time, because the possibility that retaliatory actions could significantly impair neutral computers or networks makes this option undesirable.⁸¹

Improve opportunities for U.S. companies to pursue legal action in the United States against Chinese commercial espionage. The IP Commission recommends the Economic Espionage Act (18 U.S.C. § 1831–1839) be amended to “provide a federal private right of action for trade secret theft.”⁸² Mr. Kamphausen explained, “This essentially means you can bring your own [law] suit. You don’t have to wait for the government to take one up on your behalf.”⁸³

Shift jurisdiction for all appeals in Economic Espionage Act cases to the Court of Appeals for the Federal Circuit. The IP Commission recommends Congress “make the Court of Appeals for the Federal Circuit (CAFC) the appellate court for all actions under the [Economic Espionage Act].”⁸⁴ At present, appeals in Economic Espionage Act cases are handled by a court of appeals in one of the United States’ 12 regional circuits.⁸⁵ The IP Commission writes, “The CAFC serves as the appellate court for nearly all IP-related cases, and thus has a high degree of competency on IP issues. Making the CAFC the appellate court for all [Economic Espionage Act] issues ensures a degree of continuity in judicial opinion. Moreover, it helps support the federal circuit in expanding extraterritorial enforcement.”⁸⁶

Encourage U.S. companies and individuals to bring cases of cyber theft of intellectual property to intellectual property courts in China. According to Mr. Kamphausen, “Enormous strides have been made within the Chinese legal system with regard to protection of intellectual property and then enforcement actions

**Deterring Chinese Cyber Theft against U.S. Companies—
*Continued***

once cases are brought.”⁸⁷ In his comments, he indicated to the Commission these courts may become a viable option for U.S. companies seeking recourse when their intellectual property has been stolen.

Furthermore, a variety of potential multilateral measures to deter Chinese cyber theft are under discussion, including the following:

Expand information sharing among countries regarding cyber threats. For example, countries could create an international list of “bad players” to which private companies could contribute information.⁸⁸

*Include standards for safeguarding intellectual property in negotiations of the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (T-TIP) agreements.*⁸⁹ Intellectual property rights is one of the issues partner countries are discussing in these negotiations.⁹⁰ However, the TPP negotiating parties have yet to reach consensus on this issue. They met in Tokyo in October 2013 to discuss the intellectual property chapter of the TPP.⁹¹ The United States and the European Union only recently started negotiating the T-TIP, thus discussions of intellectual property rights in this forum are in the beginning stage.⁹²

Finally, some discussions focus on improving the U.S. government’s ability to develop and implement cyber policy as necessary steps to address Chinese cyber theft. Suggestions include the following:

Appoint a Cabinet-level official to oversee an interagency process regarding the protection of intellectual property. According to the IP Commission, this step is necessary, because executive branch “efforts to protect American intellectual property will involve literally thousands of detailed actions—data gathering and research, interagency coordination, work with the private sector, coordination with Congress, and interactions with foreign government agencies.”⁹³ The IP Commission adds this undertaking will involve “expert officials across many departments and agencies.”⁹⁴

Enhance cooperation between the U.S. government and private companies. During the Commission’s roundtable, Bruce Quinn, vice president for government relations with Rockwell Automation, stressed the importance of improving cooperation between the U.S. government and the private sector to protect U.S. intellectual property from cyber intrusions. Most importantly, he said the government could provide companies with information about threats to their intellectual property as well as suggestions for protecting it. Mr. Quinn would like to see a model whereby if a company shares information about a threat with the govern-

**Deterring Chinese Cyber Theft against U.S. Companies—
Continued**

ment, the government would later provide the company with a report detailing its understanding of that threat. He said the government should provide companies with a point-of-contact for information regarding cyber threats to intellectual property.* According to Mr. Quinn, this is particularly important for small- and medium-sized companies. He explained Rockwell has “contacts with the government. . . . But these small- and medium-sized companies that funnel into us, that are critical to us being successful, they don’t have that access.” He suggested the U.S. Department of Commerce’s Foreign Commercial Service could be this point-of-contact. Under such an arrangement, the Foreign Commercial Service would have access to threat information from other U.S. government agencies. He explained, “It doesn’t have to be detailed information, but it has to be enough that they can sensitize these small- and medium-sized manufacturers to the threat and make recommendations to them if they’re looking at entering certain markets, how to best protect themselves, what to look for, what are the red flags.” He also suggested, given the government’s knowledge about cyber threats, the U.S. Defense Advanced Research Projects Agency could partner with U.S. companies to develop defensive technologies to combat cyber intrusions and then release those technologies for purchase by the public.⁹⁵

Implications for the United States

China’s cyber espionage against U.S. commercial firms poses a serious threat to U.S. business interests and competitiveness in key industries. While it is clear the economic cost of cyber espionage to the United States is significant, precise numbers are impossible to calculate. A July 2013 interim report based on an ongoing study by McAfee and CSIS estimates the annual cost of both cyber crime † and cyber espionage targeting U.S. persons and entities is between \$24 billion and \$120 billion. The report does not separate out the cost of cyber espionage, in particular, from the total amount or estimate the cost of cyber espionage originating from specific countries, such as China.⁹⁶ *The IP Commission Report* assesses the damage to the U.S. economy due to the theft of intellectual property by all means to be around \$300 billion a year. Using a range of estimates from prominent studies of this issue, the IP Commission states 50 to 80 percent of international intellectual property theft originates in China. *The IP Commission Report* lists what it appraises to be the numerous difficulties with calculating the cost of intellectual

*This proposal differs from President Obama’s February 2013 executive order regarding cybersecurity, in that the executive order is focused on information sharing between the government and critical infrastructure providers. The White House, “Executive Order—Improving Critical Infrastructure Cybersecurity” (Washington, DC: February 12, 2013). <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

†The McAfee and CSIS report defines cyber crime as the theft of financial assets, whereas the report’s examination of cyber espionage is focused on the theft of intellectual property and confidential information from companies. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), pp. 8–11.

property theft, including using surveys of a sample of companies to draw conclusions about an entire sector or a variety of sectors.*⁹⁷ General Keith Alexander, director of the NSA and commander of U.S. Cyber Command, assessed the cost to U.S. companies of intellectual property theft to be about \$250 billion a year, although not all the losses are due to Chinese activity.⁹⁸

The theft of trade secrets is a major concern for U.S. businesses with operations in China. The U.S.-China Business Council's 2013 survey of its members found they "cited trade secrets as the intellectual property (IP) issue of most concern in China."⁹⁹ If effective action to curb commercial espionage is not taken, this problem might worsen for U.S. companies. Dr. Lewis testified to the House Committee on Energy and Commerce's Subcommittee on Oversight and Investigations that although, "for China, there has been a lag of several years, perhaps as many as ten, between successful acquisition through espionage and the ability to produce competing products (be they military or civil) . . . [the] lag time between acquisition and the appearance of a competing product based on stolen technology is decreasing, as China's ability to absorb and utilize technology has increased."¹⁰⁰ This suggests the demand for U.S. intellectual property from within China could increase and with it the amount and value of intellectual property stolen.

If Chinese companies are able to duplicate technology and products using intellectual property acquired by cyber theft from U.S. companies, they may be able to compete even more effectively with U.S. companies in markets worldwide. Stealing intellectual property could allow Chinese companies to forgo some of the time and expenditure necessary for research and development.¹⁰¹ Beyond theft of proprietary information regarding technology or products, the theft of corporate e-mail correspondence or internal documents can aid Chinese companies in competitive bidding for commercial contracts.¹⁰² In each of these cases, U.S. companies might lose revenue and lay off workers or even go out of business. The theft of intellectual property, if publicized, also might lead to a drop in a company's stock value.¹⁰³ Moreover, the authors of the McAfee and CSIS report write, "Cyber espionage and crime may slow the pace of innovation, distort trade, and create social costs from job loss. This larger effect may be more important than . . . [the] actual number [of dollars lost]."¹⁰⁴

China's cyber espionage also has security implications. Information gained from intrusions into the networks of U.S. military contractors likely improves China's insight into U.S. weapon systems, enables China's development of countermeasures, and shortens China's research and development timelines for military technologies.¹⁰⁵ In addition, the same intrusions Chinese cyber actors use for espionage also could be used to prepare for offensive cyber operations. Chinese cyber actors could place latent capabilities in U.S. software code or hardware components that might be employed in a potential conflict between the United States and China.

*For the IP Commission's full assessment of the difficulties in calculating the cost of intellectual property theft, see The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), pp. 23–30. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

Conclusions

- The Chinese government is directing and executing a large-scale cyber espionage campaign against the United States and to date has successfully targeted the networks of U.S. government and private organizations, including those of DoD and private firms. These activities are designed to achieve a number of broad economic and strategic objectives, such as gathering intelligence, providing Chinese firms with an advantage over their competitors worldwide, advancing long-term research and development objectives, and gaining information that could enable future military operations.
- China has not reduced its cyber intrusions against the United States despite recent public exposure of Chinese cyber espionage in technical detail. This suggests Beijing has decided to continue its cyber campaign against the United States.
- Developments in cloud computing in China may present cybersecurity risks for U.S. users and providers of cloud computing services. The relationship between China's Ministry of State Security and the Chongqing Special Cloud Computing Zone represents a potential espionage threat to foreign companies that might use cloud computing services provided from the zone or base operations there. In addition, the plan to link 21Vianet's data centers in China and Microsoft's data centers in other countries suggests the Chinese government one day may be able to access data centers outside China through Chinese data centers.
- There is an urgent need for Washington to take action to prompt Beijing to change its approach to cyberspace and deter future Chinese cyber theft. Actions and policies under discussion include the following: passing new legislation or modifying existing legislation; changing the cost-benefit calculus of Chinese cyber actors and China's leaders through sanctions and counterintelligence tactics; undertaking multilateral measures; appointing a Cabinet-level official to oversee an interagency process regarding the protection of intellectual property; and enhancing cooperation between the U.S. government and the private sector. These would be more effective if used in combination, as they probably would lead Beijing to make only temporary or minor changes to its cyber espionage activities if used in isolation.

ENDNOTES FOR SECTION 2

1. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: February 2013), pp. 2–4, 9, 21–23. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
2. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: February 2013), p. 9. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
3. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, written testimony of Larry M. Wortzel, 113th Cong., 1st sess., July 9, 2013.
4. Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington, VA: Project 2049 Institute, November 2011), pp. 7–11. http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.
5. Danny Radron and Siobhan Gorman, "U.S., Firms Draw a Bead on Cyber-spies," *Wall Street Journal*, July 12, 2013. <http://online.wsj.com/article/SB10001424127887324694904578600041603746114.html>.
6. Craig Timberg, "Vast majority of global cyber-espionage emanates from China, report finds," *Washington Post*, April 22, 2013. http://www.washingtonpost.com/business/technology/vast-majority-of-global-cyber-espionage-emanates-from-china-report-finds/2013/04/22/61f52486-ab5f-11e2-b6fd-ba6f5f26d70e_story.html.
7. Verizon, *2013 Data Breach Investigations Report* (April 2013), pp. 5, 9, 11, 21. <http://www.verizonenterprise.com/DBIR/2013/>.
8. Tom Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *MIT Technology Review*, August 2, 2013. <http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/>.
9. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), p. 142.
10. Larry M. Wortzel, *The Dragon Extends its Reach: Chinese Military Power Goes Global* (Washington, DC: Potomac Books, 2013), p. 145.
11. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: U.S. Department of Defense, May 2013), p. 36.
12. David Alexander, "Cyber Threats Pose 'Stealthy, Insidious' Danger: Defense Chief," *Reuters*, May 31, 2013. <http://www.reuters.com/article/2013/05/31/us-usa-defense-hagel-cyber-idUSBRE94U05Y20130531>.
13. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012* (Washington, DC: U.S. Department of Defense, May 2012), p. 9.
14. David Helvey, "Press Briefing on 2012 DoD Report to Congress on *Military and Security Developments Involving the People's Republic of China*" (Washington, DC: May 18, 2012). <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5036>.
15. William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London and New York: Routledge, 2013), pp. 225–226.
16. Ministry of Foreign Affairs (China), "2013 Nian 2 Yue 19 Ri Waijiaobu Fayanren Honglei Zhuchi Lixing Jizhehui" (Ministry of Foreign Affairs Spokesperson Hong Lei Presides Over Regular Press Conference) (Beijing, China: February 19, 2013). http://www.fmprc.gov.cn/mfa_chn/fyrbt_602243/t1014798.shtml.
17. Ministry of National Defense (China), "Zhonguo Junfang Jixu Pibo Wangluo Gongji Bushi Zhize" (China's Military Continues to Refute False Accusations of "Cyber Attacks") (Beijing, China: February 20, 2013). http://news.mod.gov.cn/headlines/2013-02/20/content_4433454.htm.
18. Don Lee, "China Dismisses U.S. Accusations of Cyber-Spying," *Los Angeles Times*, May 7, 2013. <http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507>.
19. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. [http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&r=1&Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media." *Wall Street Journal*, January 31, 2013. <http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html>.](http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&r=1&Siobhan%20Gorman,%20Devlin%20Barrett,%20and%20Danny%20Yadron,%20Chinese%20Hackers%20Hit%20U.S.%20Media)
20. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&r=1&>.

21. Nicole Perlroth, "Hackers in China Attacked the Times for the Last 4 Months," *New York Times*, January 30, 2013. <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?hp&r=1&>.

22. Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media," *Wall Street Journal*, January 31, 2013. <http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html>; Craig Timberg and Ellen Nakashima, "Chinese Hackers Suspected in Attack on The Post's Computers," *Washington Post*, February 1, 2013. http://articles.washingtonpost.com/2013-02-01/business/36685685_1_chinese-hackers-cyberattacks-mandiant.

23. Siobhan Gorman, Devlin Barrett, and Danny Yadron, "Chinese Hackers Hit U.S. Media," *Wall Street Journal*, January 31, 2013. <http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html>.

24. Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013. http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi.

25. Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *Washington Post*, May 20, 2013. http://articles.washingtonpost.com/2013-05-20/world/39385755_1_chinese-hackers-court-orders-fbi.

26. Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: October 10, 2012), p. 1. <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>.

27. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

28. U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). <http://www.justice.gov/opa/pr/2013/June/13-crm-730.html>.

29. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute" (Washington, DC: Center for American Progress, June 2013). <http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/>;

U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). <http://www.justice.gov/opa/pr/2013/June/13-crm-730.html>.

30. Erin Ailworth, "Files Trace Betrayal of a Prized China-Mass. Partnership," *Boston Globe*, July 10, 2013. <http://www.bostonglobe.com/business/2013/07/09/global-chase-cracked-corporate-espionage-case/8HC7wKBJeZDkNFNSWB5dFO/story.html>; U.S. Department of Justice, "Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets" (Washington, DC: June 27, 2013). <http://www.justice.gov/opa/pr/2013/June/13-crm-730.html>.

31. Carl Sears and Michael Isikoff, "Chinese Firm Paid Insider 'to Kill My Company,' American CEO Says," *NBC News*, August 6, 2013. <http://investigations.nbcnews.com/news/2013/08/06/19566531-chinese-firm-paid-insider-to-kill-my-company-american-ceo-says?lite>.

32. Erin Ailworth, "Files Trace Betrayal of a Prized China-Mass. Partnership," *Boston Globe*, July 10, 2013. <http://www.bostonglobe.com/business/2013/07/09/global-chase-cracked-corporate-espionage-case/8HC7wKBJeZDkNFNSWB5dFO/story.html>.

33. Melanie Hart, "Criminal Charges Mark New Phase in Bellwether U.S.-China Intellectual Property Dispute" (Washington, DC: Center for American Progress, June 2013). <http://www.americanprogress.org/issues/china/news/2013/06/27/68339/criminal-charges-mark-new-phase-in-bellwether-u-s-china-intellectual-property-dispute/>.

34. Reuters, "U.S., China Agree To Work Together on Cyber Security," April 13, 2013. <http://www.reuters.com/article/2013/04/13/us-china-us-cyber-idUSBRE93C05T20130413>.

35. BBC News, "US-China Cyber Security Working Group Meets," July 8, 2013. <http://www.bbc.co.uk/news/world-asia-china-23177538>.

36. U.S. Department of State, "U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track" (Washington, DC: July 12, 2013). <http://www.state.gov/r/pa/prs/ps/2013/07/211861.htm>.

37. House Foreign Affairs Committee, Subcommittee on Asia and the Pacific, *Hearing on Asia: The Cybersecurity Battleground*, written testimony of James A. Lewis, 113th Cong., 1st sess., July 23, 2013.

38. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (June

7, 2013), p. 8. [https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/\\$FILE/A%2068%2098.pdf](https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf).

39. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (June 7, 2013), p. 8. [https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/\\$FILE/A%2068%2098.pdf](https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf).

40. James Crawford, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) (New York: United Nations Audiovisual Library of International Law, 2012). <http://legal.un.org/avl/ha/rsiwa/rsiwa.html>.

41. Jen Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts On Cyber Issues," (Washington, DC, June 7, 2013). <http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm>; Philip Rucker and Ellen Nakashima, "Obama Begins Summit With Xi as China Agrees to Cyber Framework," *Washington Post*, June 7, 2013. http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi.

42. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

43. Adam Segal, "China, International Law, and Cyberspace," *Asia Unbound*, October 2, 2012. <http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/>; Timothy Farnsworth, "Expert Group Coalesces on Cyberspace," *Arms Control Today*, July/August 2013. http://www.armscontrol.org/act/2013_0708/Expert-Group-Coalesces-on-Cyberspace; and Philip Rucker and Ellen Nakashima, "Obama Begins Summit With Xi as China Agrees to Cyber Framework," *Washington Post*, June 7, 2013. http://articles.washingtonpost.com/2013-06-07/politics/39823657_1_president-obama-chinese-president-xi-jinping-obama-and-xi.

44. Lana Lam, "Edward Snowden: US Government Has Been Hacking Hong Kong and China for Years," *South China Morning Post* (Hong Kong), June 14, 2013. <http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china?page=all>.

45. Chris Buckley, "Chinese Defense Ministry Accuses U.S. of Hypocrisy on Spying," *New York Times*, June 27, 2013. http://www.nytimes.com/2013/06/28/world/asia/chinese-defense-ministry-accuses-us-of-hypocrisy-on-spying.html?_r=0.

46. The White House, "Press Briefing by National Security Advisor Tom Donilon" (Washington, DC: June 8, 2013). <http://www.whitehouse.gov/the-press-office/2013/06/09/press-briefing-national-security-advisor-tom-donilon>; Bloomberg TV, "Obama: Blunt Conversation with China on Hacking," June 18, 2013. <http://www.bloomberg.com/video/obama-blunt-conversation-with-china-on-hacking-EvHfGSCRsGYoAVpMiuCmA.html>; and The White House, "Readout of the President's Meeting with the Co-Chairs of the U.S.-China Strategic and Economic Dialogue" (Washington, DC: July 11, 2013). <http://www.whitehouse.gov/the-press-office/2013/07/11/readout-president-s-meeting-co-chairs-us-china-strategic-and-economic-di>.

47. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

48. Mike Rogers and C.A. Dutch Ruppertsberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Washington, DC: House Permanent Select Committee on Intelligence, October 8, 2012), pp. vi, 1, 3.

49. Christopher Joye, "Transcript: Interview with Former CIA, NSA Chief Michael Hayden," *Australian Financial Review*, July 19, 2013. <http://www.afr.com/p/national/transcript-interview-with-former-KnS7JDIrw73GWlljxA7vdK>.

50. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," *Bloomberg*, August 18, 2013. <http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html>.

51. Tom Pullar-Strecker, "Huawei Founder Gives First Ever Media Interview," *Fairfax Media* (Auckland), May 9, 2013. <http://www.stuff.co.nz/business/industries/8651260/Huawei-CEO-gives-first-ever-interview>.

52. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," *Bloomberg*, August 18, 2013. <http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html>.

53. U.S. Customs and Border Protection, "Notice of Issuance of Final Determination Concerning Video Teleconference Server," September 11, 2013. http://www.ofr.gov/OFRUpload/OFRData/2013-22765_PI.pdf.

54. Kathleen Miller, "China Video Tools for U.S. Help Spurs Spy Anxiety," Bloomberg, August 18, 2013. <http://www.bloomberg.com/news/2013-08-19/china-video-tools-for-u-s-with-american-help-spurs-spy-anxiety.html>.

55. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2011* (Public Law 111-383), 111th Cong., 2nd sess., January 7, 2011. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf>.

56. Special Assistant to the DoD Chief Information Officer, Office of the Assistant Secretary of Defense for Legislative Affairs, e-mail interview with Commission staff, May 28, 2013.

57. Special Assistant to the DoD Chief Information Officer, Office of the Assistant Secretary of Defense for Legislative Affairs, e-mail interview with Commission staff, May 28, 2013.

58. IBM, "What is Cloud Computing?" <http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html>. For a fuller explanation of China's efforts in this arena, see Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013).

59. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), pp. 32-34.

60. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), pp. 37.

61. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 37.

62. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 39.

63. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 43.

64. Leigh Ann Ragland et al., *Red Cloud Rising: Cloud Computing in China* (Vienna, VA: Defense Group Inc. for the U.S.-China Economic and Security Review Commission, September 2013), p. 38.

65. Dan McWhorter, "APT1 Three Months Later—Significantly Impacted, Though Active & Rebuilding," *M-union*, May 21, 2013. <https://www.mandiant.com/blog/apt1-months-significantly-impacted-active-rebuilding/>; Richard Bejtlich (chief security officer at Mandiant), telephone interview with Commission staff, August 21, 2013.

66. Richard Bejtlich (chief security officer at Mandiant), telephone interview with Commission staff, August 21, 2013.

67. Danny Radron and Siobhan Gorman, "U.S., Firms Draw a Bead on Cyber-spies," *Wall Street Journal*, July 12, 2013. <http://online.wsj.com/article/SB10001424127887324694904578600041603746114.html>.

68. Richard Bejtlich (chief security officer at Mandiant), e-mail interview with Commission staff, November 12, 2013.

69. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

70. U.S. Senate, *Deter Cyber Theft Act* (S. 884), 113th Cong., 1st sess. (introduced in Senate May 7, 2013). <http://thomas.loc.gov/cgi-bin/query/z?c113:S.884>.

71. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 66. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

72. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

73. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

74. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013); *Economist*, "Admit nothing and deny everything," June 8, 2013. <http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyber-attacks-makes-one>.

75. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).

76. John Reed, "DoD Says Don't Worry About Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy*, May 28, 2013. <http://killerapps.foreignpolicy.com/>

- [posts/2013/05/28/dod_says_dont_worry_about_hackers_accessing_key_us_weapons_designs.](#)
77. John Reed, "DoD Says Don't Worry About Hackers Accessing Key U.S. Weapons Designs," *Foreign Policy*, May 28, 2013. [http://killerapps.foreignpolicy.com/posts/2013/05/28/dod_says_dont_worry_about_hackers_accessing_key_us_weapons_designs.](http://killerapps.foreignpolicy.com/posts/2013/05/28/dod_says_dont_worry_about_hackers_accessing_key_us_weapons_designs)
78. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 81. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
79. Cisco, "Data Loss Prevention." <http://www.cisco.com/en/US/netsol/ns895/index.html>.
80. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
81. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 81. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
82. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 5.
83. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
84. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 5. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
85. Trade Secrets Institute, "Cases from Economic Espionage Act" (Brooklyn, NY: Brooklyn Law School). <http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espionage-act>; United States Courts, "Courts of Appeals." <http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/CourtofAppeals.aspx>.
86. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 74. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
87. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
88. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
89. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
90. European Commission, "EU and US conclude first round of TTIP negotiations in Washington," July 12, 2013. <http://trade.ec.europa.eu/doclib/press/index.cfm?id=941>; Shawn Donnan and Ben Bland, "TPP leaders say 'significant progress made.'" *Financial Times*, October 8, 2013. <http://www.ft.com/intl/cms/s/0/fdfe4b36-2fe5-11e3-9ecc-00144feab7de.html?siteedition=intl#axzz2ho8IOsYP>.
91. Kyodo News (Tokyo), "TPP Countries To Speed Up Talks On Intellectual Property: Official," October 28, 2013. <http://e.nikkei.com/e/fr/tnks/Nni20131028D28JF572.htm>.
92. European Commission, "EU and US conclude first round of TTIP negotiations in Washington," July 12, 2013. <http://trade.ec.europa.eu/doclib/press/index.cfm?id=941>.
93. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 63. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
94. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 63. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
95. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013).
96. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 5. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.
97. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), pp. 2-3, 23. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
98. Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012. http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

99. U.S.-China Business Council, "Shanghai: Battling Trade Secrets and Data Theft in China." <http://www.uschina.org/battling-trade-secrets-and-data-theft-china>.

100. House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, written testimony of James A. Lewis, 113th Cong., 1st sess., July 9, 2013.

101. Mike McConnell, Michael Chertoff, and William Lynn, "Cyber Thievery is National Policy—And Must be Challenged," *Wall Street Journal*, January 27, 2012. <http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html>.

102. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington, DC: July 11, 2013); James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 10. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

103. The Commission on the Theft of American Intellectual Property, *The IP Commission Report* (Seattle, WA: The National Bureau of Asian Research, May 2013), p. 10. http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

104. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: CSIS, July 22, 2013), p. 5. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

105. Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies," *Washington Post*, May 27, 2013. http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

SECTION 3: CHINA'S MARITIME DISPUTES

Introduction

This section provides an overview of China's East China Sea and South China Sea disputes, covering the drivers of Beijing's approach to the disputed waters, the means by which China is asserting sovereignty in those areas, the risks of escalation or miscalculation at sea, and the consequential dangers of political or military escalation. It is based on witness testimonies from Commission hearings; information from the Commission's fact-finding trips to China, Japan, and Taiwan; and additional research. This section primarily focuses on the East China Sea; the South China Sea was covered in detail in chapter 3, section 1, of the Commission's 2012 Annual Report.

Maritime Dispute Overview

Peter Dutton, professor and director of the China Maritime Studies Institute at the U.S. Naval War College, testified to the Commission that China's overall interests and objectives in the East and South China Seas include:

*... enhancing China's sense of national security, acquiring control over the region's living and non-living maritime resources, and restoring China's place of pre-eminence in the East Asian regional order ... Additionally, consolidating Chinese state power over the offshore islands and regional seas serves the Communist Party's interest in maintaining internal political credibility by delivering to the Chinese people what they believe is rightfully their own.*¹

Although sovereignty disputes in the East and South China Seas are not new, China's growing diplomatic, economic, and military clout is improving China's ability to assert its interests. It is increasingly clear that China does not intend to resolve the disputes through multilateral negotiations or the application of international laws and adjudicative processes but instead will use its growing power in support of coercive tactics that pressure its neighbors to concede China's claims.

East China Sea Dispute Background

The East China Sea dispute involves China, Japan, and Taiwan (see figure 1).^{*} The dispute can be divided into two distinct issues: territorial sovereignty over the Senkaku Islands (known as Diaoyu Dao in China, and Diaoyutai in Taiwan), and demarcation of maritime zones, which has implications for natural resource rights.

^{*}For a discussion of Taiwan's role in China's maritime disputes, see chapter 3, section 2, of this Report, "Taiwan."

China's most intense dispute in this area relates to territorial sovereignty over the Senkaku Islands, eight uninhabited islets that lie approximately 120 nautical miles (nm) northeast of Taiwan, and 240 nm southwest of Japan's Okinawa Island. China and Taiwan rely on a historical foundation as far back as the Ming Dynasty (1368–1644) to justify their claims to the islands. According to China's official narrative, Japan "secretly 'included' Diaoyu Dao in its territory at the end of the Sino-Japanese War of 1894–1895. Japan then forced China to sign the unequal Treaty of Shimonoseki," ceding the Senkaku Islands and Taiwan to Japan.²

Japan administers the Senkaku Islands and asserts there is no territorial dispute over the islands. When Japan made an official declaration incorporating the Senkaku Islands into Japanese territory in 1895, it considered them uninhabited land without an owner. The United States administered the islands following the 1951 Treaty of San Francisco officially concluding World War II until the 1971 Okinawa Reversion Treaty came into force. This treaty transferred administrative rights over the Senkaku Islands to Japan while maintaining U.S. neutrality on the ultimate sovereignty of the islands.³ Japan argues China did not express an interest in the islands until a 1968 United Nations (UN) study suggested the possibility of petroleum resources in the East China Sea.⁴

The Japanese government's September 2012 purchase of three of the Senkaku Islands from a private Japanese owner angered China, sparking an escalation in tensions between China and Japan.⁵ Beijing immediately responded by issuing a Government Statement, its highest-level diplomatic document, which for the first time includes map coordinates to its claims in the East China Sea.[†] Later that month, China's State Council released a white paper on the Senkakus, its first ever on a territorial dispute, which stated the "Diaoyu Dao is China's inherent territory in all historical, geographical, and legal terms, and China enjoys indisputable sovereignty over Diaoyu Dao."⁶

A separate but equally important dispute among China, Japan, and Taiwan is over rights and interests (including natural resource extraction) involving maritime demarcation of overlapping exclusive economic zones (EEZ) within the East China Sea. The dispute—which primarily concerns the Chunxiao (Shirakaba in Japanese) Gas Field—is mainly a result of differing interpretations of the United Nations Convention on the Law of the Sea (UNCLOS). Among many other provisions, UNCLOS allots nations an EEZ out to 200 nm from their coastal baselines.[‡] Although a coastal nation

*For more information on the background and domestic aftermath of the Senkaku Islands purchase in China, reference the East China Sea subsection in chapter 2, section 1, of the Commission's 2012 Annual Report, "China's Impact on U.S. Security Interests," pp. 133–135.

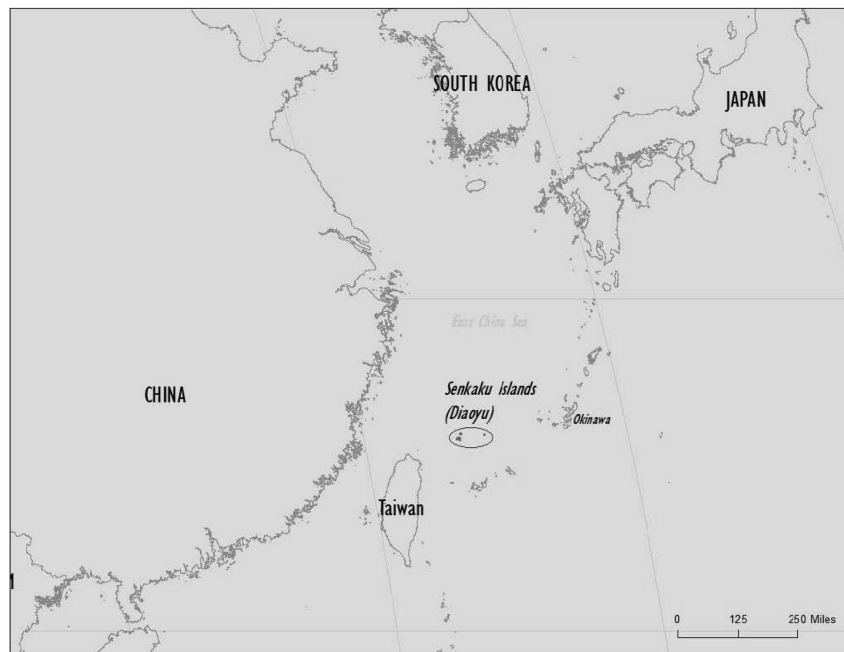
†Government Statements represent China's highest-level, most authoritative message. Prior to this incident, China had only twice issued a Government Statement—once regarding the Sino-Vietnamese War and once regarding the 1999 destruction of China's embassy in Belgrade during U.S. bombing operations. Open Source Center, "China Shows No Sign of Easing Tough Public Posture on Senkakus," September 14, 2012. OSC ID: CPF20120914534001. <http://www.opensource.gov>; J. Ashley Roach, "China's Straight Baseline Claim: Senkaku (Diaoyu) Islands," *American Society of International Law Insights*, February 13, 2013. <http://www.asil.org/pdfs/insights/insight130213.pdf>.

‡One nautical mile is approximately equal to 1.15 statute miles. Therefore, 200 nautical miles is roughly 230.16 statute miles.

cannot claim full sovereignty in an EEZ, it does have sovereign rights to explore, exploit, and protect natural resources, including fisheries, in this zone.⁷ UNCLOS also provides similar rights over natural resources, with the exception of fishing, in an extended continental shelf zone up to 150 nm beyond a country's EEZ, subject to certain restrictions based on seafloor geography.⁸

Because the maritime distance between China and Japan in the East China Sea is less than 400 nm, neither China nor Japan can claim a full EEZ in this region. Japan proposes a median line between the two countries as an attempt to divide EEZ rights evenly. China claims an extension of its continental shelf eastward past the median line to the Okinawa Trough and in December 2012 formalized its position in a claim submission to the United Nations.⁹

Figure 1: The East China Sea



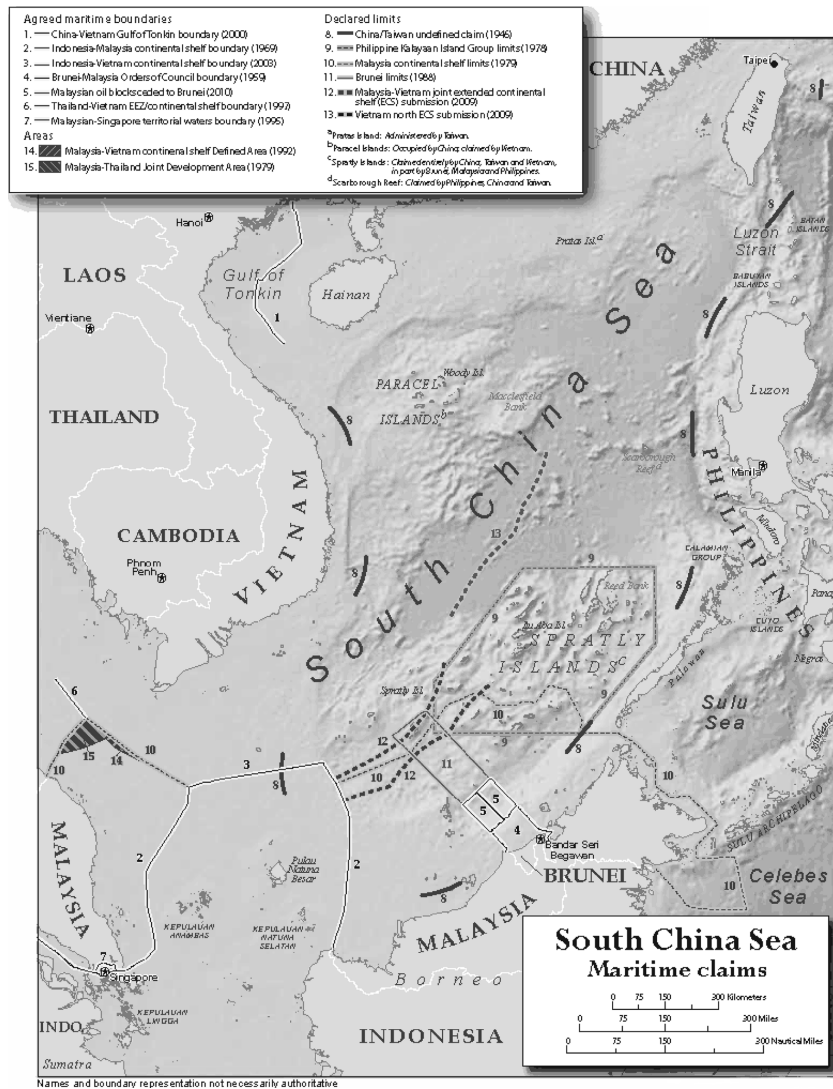
Source: Mark Manyin, Senkaku (Diaoyu/Diaoyutai) Islands Dispute: U.S. Treaty Obligations (Washington, DC: Congressional Research Service, January 2013).

South China Sea Dispute Background

Six parties claim the South China Sea in part or in full: China, Taiwan, Vietnam, the Philippines, Malaysia, and Brunei. Beijing denotes its claim on its South China Sea maps using a nine-dash line, with an additional dash off the coast of Taiwan to demonstrate its claim over Taiwan (see figure 2). Also in dispute are two sets of island groups: the Paracel Islands, located in the northern part of the sea, and the Spratly Islands, a widespread collection of approximately 200 islands, islets, rocks, and reefs located in the southern part of the South China Sea. China occupies the Paracel

Islands, though Taiwan and Vietnam also lay claim to them. While all claimants except Brunei have established military outposts in the Spratly Islands, China and Vietnam occupy the greatest number of outposts.* For a comprehensive discussion of the South China Sea dispute, see chapter 3, section 1, of the Commission's 2012 Annual Report, "China and the South China Sea."

Figure 2: The South China Sea



Source: U.S. State Department. From U.S. Energy Information Administration, *South China Sea* (Washington, DC: February 2013). <http://www.eia.gov/countries/regions-topics.cfm?fips=SCS>.

* For more information on Taiwan's claims and outposts and for another map depiction of the South China Sea, see chapter 3, section 2, of this Report, "Taiwan."

China's Overall Approach to Maritime Disputes

At the Commission's hearing on China's maritime disputes, two longtime China watchers concluded that China is seeking to change the status quo in its favor in both the East and South China Seas. Rear Admiral Michael McDevitt, USN (Retd.), senior fellow at CNA Center for Naval Analysis, said in testimony to the Commission that China has taken a "proactive approach toward creating a new, [more] favorable status quo" with regard to its maritime disputes. He assessed Beijing has been more assertive since 2012, offering rival claimants the choice of either facing the brunt of Chinese power as a result of challenging Chinese claims or benefitting from economic and political rewards for moderating their positions or even acquiescing to China's claims.¹⁰

Michael Swaine, senior associate at the Carnegie Endowment for International Peace, emphasized in his testimony that Beijing has in some instances "responded in a deliberately escalatory manner" to perceived attempts by China's rival claimants to secure territorial gains in the disputed waters, "seeking to create a new status quo in its favor or to undertake a more muscular or aggressive action in order to convey resolve and deter further escalation by others."¹¹ For example, Beijing appears to have calculated that Japan's purchase of the Senkaku Islands provided a justification to deploy a regular maritime presence supporting a new status quo in China's favor.¹²

Chinese official statements and use of maritime law enforcement rather than military forces suggest Beijing prefers to avoid direct military conflict over its maritime disputes and rely on the shift in the balance of regional power in its favor to resolve its maritime disputes in the long term.¹³ China probably judges that as a result of its growing power and influence vis-à-vis other claimants to the East and South China Seas, time is on its side with regard to consolidating control over its maritime claims.

Drivers of China's Approach to Maritime Disputes

Nationalism

The new Chinese Communist Party (CCP) leadership has affirmed that it intends to continue governing China without resort to elections or other democratic processes, and the CCP has long been aware that the absence of democratic legitimacy tends to undermine the stability of its rule. As a result, the CCP places a high priority on legitimizing itself by convincing the Chinese people that it is delivering economic growth, a better quality of life, and an assertion of China's ascendancy regionally and globally.

In fact, Beijing has long used the education system and media to cultivate an awareness of China's victimization during what China calls its century of humiliation from the mid-19th to the mid-20th centuries.¹⁴ By promoting a sense of grievance among the Chinese people, and then aggressively asserting China's claims against its neighbors, the CCP shifts attention away from the authoritarian nature of its rule and toward its role as the champion of China's interests in the region.

China not only takes an aggressive stance in the region to satisfy the nationalistic impulse it has promoted; it also uses nationalism

domestically to support its regional claims. Jessica Chen Weiss, assistant professor of political science at Yale University, testified to the Commission: “The Chinese government has allowed nationalist street demonstrations when it wants to demonstrate resolve to signal that China will not budge on [an] issue. Just as the [U.S.] president can point to Congress and say his hands are tied, so can the Chinese leadership point to nationalist fervor and say that they can’t compromise or else protestors will turn against them.”¹⁵

For example, Beijing permitted large-scale, anti-Japanese demonstrations in the fall of 2012 following the Japanese government’s purchase of several of the Senkaku Islands. Demonstrations in China’s second- and third-tier cities even became destructive, damaging storefronts of Japanese companies, such as Toyota and Panasonic.¹⁶

On the other hand, the Chinese government suppresses popular nationalism if it believes doing so will help it achieve its diplomatic objectives.¹⁷ For example, in a move attributed to Beijing, the Hong Kong government in August 2013 prevented a group of anti-Japan activists from sailing to the Senkaku Islands as they did in 2012 to mark the anniversary of Japan’s World War II surrender.¹⁸ Beijing likely judged popular Chinese animosity toward Japan threatened a potentially volatile public backlash that it might not be able to manage or exploit to its advantage. However, as Dr. Weiss testified, suppressing nationalist sentiment is “costly for the Chinese government, which has often been accused [by its people] of being both unpatriotic and undemocratic in suppressing nationalist sentiment.”¹⁹

Sovereignty and “Core Interests”

China’s view of “indisputable sovereignty” over its maritime claims underlies its overall policy approach to the East and South China Seas.²⁰ As tensions involving China’s maritime disputes in the East China Sea and South China Sea have grown since 2009, official and unofficial Chinese sources indicate China views the East and South China Seas as central to its “core interests,” which authoritative Chinese speeches and documents define as (1) national security; (2) sovereignty and territorial integrity; and (3) economic and social sustained development.²¹ Beijing makes core interest declarations to signal to other countries that China is unwilling to compromise on particular policy issues and to imply that China would use force to defend its core interests. These declarations usually relate to matters regarding China’s territorial sovereignty, such as Taiwan, Tibet, and Xinjiang.²²

China appears to have overtly linked the South China Sea and East China Sea to China’s core interests in recent years.*²³ Japanese commentators expressed concern that the designation of the Senkaku Islands as a core interest in April signaled a shift in Bei-

* According to Japanese press reports, a Chinese Ministry of Foreign Affairs spokesperson stated in a regular press briefing that “[t]he Diaoyu [Senkaku] Islands are about sovereignty and territorial integrity. Of course, it’s China’s core interest.” An official Ministry of Foreign Affairs transcript quotes the spokesperson as saying the issue of the contested islands “touches on” China’s core interests. Kyodo, “China Says Senkaku Islands are its ‘Core Interest,’” April 26, 2013. OSC ID: JPP20130426969071. <http://www.opensource.gov>; Open Source Center, “China-Japan—Video of PRC Remarks on Senkakus as ‘Core Interest’ Differs from Official Transcript,” May 7, 2013. OSC ID: CPP20130507358001. <http://www.opensource.gov>.

jing's approach to the maritime dispute and indicated China "will make no concessions on the islets."²⁴ Subsequent official Chinese statements have not clarified the status of the islands, allowing Beijing to maintain flexibility in its approach to the dispute, prevent any domestic accusations that China is adopting a weaker stance, and deny that it is taking unilateral actions or escalating tensions.²⁵

Economic Development

China also views the East and South China Seas as central to its economic development, due to their resource potential and significant roles as maritime transit routes. Though nationalism has a stronger pull on China's foreign policy-making levers with regard to its maritime disputes, natural resources are significant because they galvanize popular nationalist sentiment.²⁶

Oil and Gas Resources: China's surging economy has made the country increasingly dependent on oil and gas to supply its growing industrial and manufacturing base. However, hydrocarbon reserves in the East and South China Seas would provide only modest relief to the heavy energy demands of many of the surrounding Asian economies, according to Lloyd Thrall, project associate at the RAND Corporation.²⁷ Additionally, the financial feasibility of exploiting oil and gas reserves in these areas is limited at best. In the South China Sea, the risk and cost of recovering deepwater oil and gas in contested waters prone to unusually strong currents and tropical storms heavily outweighs the minimal benefit of yet-to-be-proven hydrocarbons.²⁸ Nevertheless, the speculation and perceived economic value of natural resources in both seas fuels the narrative of competition and sovereignty by the respective claimants.²⁹

Maritime Trade Routes: The East and South China Seas play central roles in the transport of oil and gas to China's coastal regions, which serve as the engines of China's economic growth.³⁰ According to the U.S. Energy Information Administration, almost a third of the world's crude oil passes through the South China Sea, with about 15 percent of this volume moving on to Northeast Asia and the East China Sea.³¹ Additionally, over half of the world's traded liquefied natural gas (LNG) passes through the South China Sea. China's reliance on this trade route is projected to grow significantly in the coming two decades due to increasing LNG consumption. As Steven Lewis, fellow and professor at Rice University, testified to the Commission: "The future economic growth of China's most prosperous cities and provinces is one heavily tied to massive fleets of LNG carriers (with four or five times the number of vessels used today)" transiting the East and South China Seas.³²

Fisheries: According to Mr. Thrall, "Fishermen in East and Southeast Asia are potent national symbols ... to have fishermen denied their livelihood in areas perceived as historical fishing grounds, or, worse yet, detained or facing violence can strike deeply discordant notes" within China.³³ This dynamic helps explain the nationalist sentiment in China that followed the detention of the captain of a Chinese fishing trawler upon his collision with a Japanese Coast Guard (JCG) vessel in September 2010. Similar senti-

ments are prevalent across the region; the death of a Taiwan fisherman in May 2013, a result of the Philippine Coast Guard firing shots at a Taiwan fishing boat in disputed fishing grounds, set off nationalist outpourings across Taiwan. The incident led to three months of strained relations between Taiwan and the Philippines that ended only after Manila offered an official apology, agreed to pay compensation to the victim's family, and recommended homicide charges for the Philippine Coast Guard personnel who opened fire on the Taiwan fishing boat.³⁴ See chapter 3, section 2, of this Report, "Taiwan," for full coverage of the Taiwan-Philippine row.

Advancing Maritime Claims in Regional and Multilateral Organizations

The multilateral nature of the South China Sea dispute, as opposed to the generally bilateral nature of the East China Sea dispute, diffuses negotiating power among multiple claimants, giving China relatively less influence in the multilateral dispute resolution process. China as a result seeks to "divide and conquer" by negotiating the issue on a bilateral basis rather than under the auspices of the Association of Southeast Asian Nations (ASEAN). At the ASEAN Regional Forum Foreign Ministers' Meeting in July 2013, Chinese Foreign Minister Wang Yi underscored this approach: "The South China Sea issue is not an issue between China and ASEAN. It is only an issue between China and a small number of Southeast Asian countries."³⁵ In 2013, there have been two significant efforts in multilateral venues seeking to resolve South China Sea disputes; China has stalled progress in one and refused to participate in the other.

South China Sea Code of Conduct negotiations: Chinese obstructionism and efforts to exploit disunity among Southeast Asian nations was a factor in stalled progress toward a binding Code of Conduct in the South China Sea. China and ASEAN in 2002 signed a Declaration on the Conduct of Parties in the South China Sea that laid the groundwork for an eventual Code of Conduct. However, despite agreeing to "work, on the basis of consensus, towards the eventual attainment" of a "code of conduct in the South China Sea [that] would further promote peace and stability in the region," Beijing remains circumspect on ASEAN calls for formal, substantive Code of Conduct talks.*³⁶ During an August 2013 multi-country visit to Southeast Asia, Foreign Minister Wang emphasized patience in what he described would be a long-term process toward concluding a Code of Conduct.³⁷

Philippines-initiated arbitration over South China Sea claims: Manila surprised many observers in January 2013 when it initiated UNCLOS-based arbitration challenging China's nine-dash line and maritime claims in the South China Sea. Beijing has rejected the arbitral process as "manifestly unfounded" under UNCLOS and declined to participate.³⁸ In an official Foreign Ministry statement responding to the arbitration, Beijing denounced the Philippines'

*For an additional discussion of the Declaration on Conduct and the Code of Conduct, reference chapter 3, section 1, of the Commission's 2012 Annual Report, "China and the South China Sea," p. 237.

“illegal occupation” of China’s claimed islands and reefs and argued the arbitral process counteracts ongoing bilateral negotiations that would peacefully resolve the South China Sea issue.³⁹ However, China’s refusal to participate in the arbitration has not prevented the formation of an arbitral tribunal or delayed the proceedings. A five-judge tribunal in the Hague is expected to consider Manila’s arguments following their submission in March 2014 and is likely to conclude proceedings by mid-2015.*⁴⁰

Political tension is particularly pronounced between China and the Philippines due to China’s view that the Philippines has internationalized the South China Sea disputes.⁴¹ In August 2013, official Chinese press signaled displeasure with the Philippines, seemingly for instituting arbitration to draw international attention to the lack of progress on a Code of Conduct: “. . . certain countries are deliberately creating an issue of the ‘Code of Conduct’ and are not genuinely concerned about the ‘Code’ but instead want to use this kind of hyping to multilateralize and internationalize South China Sea issues.”⁴²

Legal and Administrative Assertions of Maritime Sovereignty

Since late 2012, China has stepped up its use of a number of legal and administrative methods to assert sovereignty over its claims in the East and South China Seas, including the following:

- After the Japanese Senkaku purchase in September 2012, Beijing published its claim to the disputed islands in an official Government Statement “on the Baselines of the Territorial Sea of Diaoyu Dao and Its Affiliated Islands” and submitted these claims to the UN.⁴³ Japan, which does not officially recognize a dispute over the islands, countered with its position that China’s submission was “totally unacceptable and legally invalid.”⁴⁴ The United States also has protested China’s claims, calling them “improperly drawn.”⁴⁵
- In 2012, China introduced a new passport design that has a watermark of a national map that includes popular tourist sites in Taiwan, its nine-dash line around the South China Sea, and border areas disputed with India as part of its territory. Countries disputing the depiction of China’s territory denounced China’s new passports, and some are not stamping the new passports and instead are issuing separate visa sheets.⁴⁶
- Hainan Province, China’s southernmost province, issued new maritime regulations in late 2012. The regulations, which are

*The selected arbitrators include Judge Thomas Mensah (Ghana), Judge Jean-Pierre Cot (France), Judge Stanislaw Pawlak (Poland), Professor Alfred Soons (the Netherlands) and Judge Rüdiger Wolfrum (Germany). Judge Thomas Mensah is serving as the arbitral panel’s president. According to Annex VII of UNCLOS, each of the parties in arbitration may select one judge. The remaining three judges are in normal circumstances to be selected by agreement between the parties. Because of China’s refusal to participate, the Philippines selected Judge Wolfrum, and the president of the International Tribunal on the Law of the Sea appointed the four remaining arbitrators. Luke Eric Peterson, “Philippines-China UNCLOS arbitration moving forward without Chinese participation,” Kluwer Arbitration Blog, August 28, 2013. <http://kluwerarbitrationblog.com/blog/2013/08/28/an-update-on-the-philippines-china-unclos-arbitration/>.

applicable to the 12 nm territorial waters within Hainan Province's announced baselines, include a provision allowing China to board, inspect, and expel foreign vessels "illegally" entering Chinese waters.⁴⁷ According to Wu Shicun, director of the Hainan Foreign Affairs Office and president of China's National Institute for South China Sea Studies, the provision is designed to curb Vietnamese fishing activity near the Paracel Islands.⁴⁸

- China's official Sinomaps Press issued a new national map in January 2013 that includes China's South China Sea claims. The new map depicts the entire South China Sea on the same scale as mainland China, rather than using insets to illustrate China's claimed island groups. The map also includes a dash southeast of Taiwan delineating China's claim over Taiwan, bringing China's well-known nine-dash line claim in the South China Sea to ten dashes. Although official Chinese maps have included the tenth dash for at least the past two years, its larger-scale incorporation into the newest version of an official Chinese map raised concerns among China's neighbors in both the East and South China Seas.⁴⁹ One Sinomaps editor said the changes in presentation served to "elevate the [Chinese] peoples' consciousness of national territory and safeguard China's maritime rights and interests."⁵⁰

Maritime Law Enforcement Assertions of Maritime Sovereignty

China's maritime law enforcement agencies since 2009 have played an increasing role as the frontline actors in staking and enforcing China's maritime claims.⁵¹ Beijing likely sees this approach as less provocative than the use of the PLA Navy and a means to demonstrate de facto governance over its territorial claims. Nevertheless, robust and near-constant deployments of increasingly capable maritime law enforcement vessels, with the PLA Navy often deployed nearby, effectively serve as coercive policy instruments in the East and South China Seas.⁵²

Since 2012, China has begun to "[respond] to challenges to its claims with an enhanced physical presence to bolster China's position and deter any further challenges," according to M. Taylor Fravel, associate professor of political science at the Massachusetts Institute of Technology. "These responses suggest an even greater willingness to pursue unilateral actions to advance its claims." Dr. Fravel further notes that this activity is a recent departure from what had for several decades been a pattern of Chinese restraint with regard to the presence of ships and aircraft in disputed waters.⁵³ Several other analysts have observed this change in China's approach to island disputes since the 2012 Scarborough Reef standoff, which began with a confrontation between China and the Philippines over the fishing activities of several Chinese fishing vessels at the reef, located in the South China Sea.*⁵⁴ Both countries had previously fished in Scarborough Reef despite disputing its

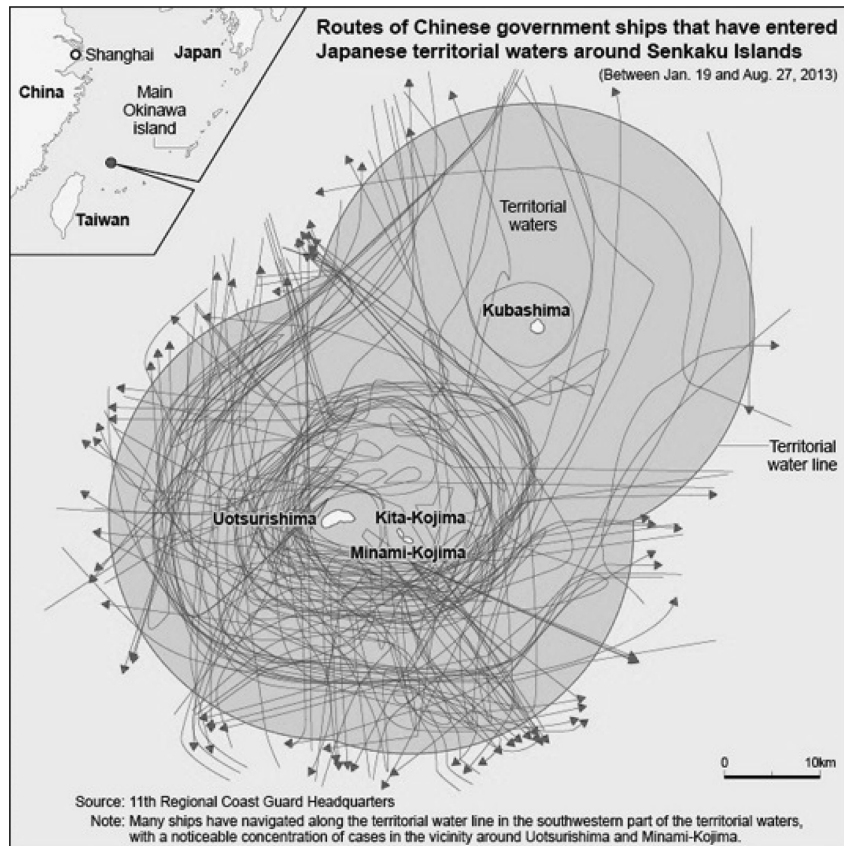
* For more information about the Scarborough Reef standoff, see chapter 3, section 1, of the Commission's 2012 Annual Report, "China and the South China Sea," p. 231–233.

territoriality. Over the course of the months-long standoff, China established physical control over the reef by patrolling the vicinity with maritime law enforcement vessels and roping off the reef's entrance to prevent Philippine vessels from operating there.⁵⁵ At the time of this Report's publication, China continues to maintain de facto control over the reef.⁵⁶

China has applied similar tactics in Second Thomas Shoal, a coral reef in the South China Sea approximately 105 nm west of Palawan Island, Philippines. The Philippines in early May 2013 reported a PLA Navy vessel escorting two Chinese maritime law enforcement ships and approximately 30 fishing boats in the shoal. The Philippines maintains a regular presence on Second Thomas Shoal of approximately 12 marines aboard the *BRP Sierra Madre*, a World War II-era U.S. tank landing ship that the Philippine Navy deliberately ran aground on the shoal in 1999 to stake its territorial claim.⁵⁷ China frames this "illegal occupation" of Chinese territory as justification for its enhanced patrols in the waters surrounding Second Thomas Shoal.⁵⁸

The Commission learned in meetings with the JCG that PLA Navy and Chinese maritime law enforcement activity near the Senkaku Islands, previously irregular and sporadic, increased sharply following Japan's Senkaku Islands purchase. Official Chinese press appears to confirm the purchase marked a turning point for China's maritime operations, after which Chinese government ships maintained a near-persistent presence near the disputed isles. (See figure 3 for a depiction of this operational state based on JCG data.)⁵⁹

Figure 3: Routes of Chinese Government Ships Near Senkaku Islands from January 19, 2013 to August 27, 2013



Source: *Asahi Shimbun* (Tokyo), "INSIGHT: Japan, China still far apart in mending ties 1 year after purchase of Senkakus," September 11, 2013. http://ajw.asahi.com/article/behind_news/AJ201309110069.

Japan Reconsiders Self-Defense in the East China Sea

The ongoing domestic debate over whether Tokyo should revise its constitution to expand the circumstances for self-defense was a prominent theme of the Commission's fact-finding trip to Japan this year. Japan remains divided on the issue of revising a constitutional provision renouncing war and preventing the maintenance of a military force.⁶⁰ In meetings with a group of retired Japan Self-Defense Force and JCG senior officers, the Commission learned that such a revision could, for example, allow the Japan Self-Defense Force to employ arms in the event of intrusion into Japan's territorial waters by foreign government vessels. The retired senior officers further explained that under the current constitution, a lengthy legal process would precede

**Japan Reconsiders Self-Defense in the East China Sea—
*Continued***

any decision by Tokyo to exercise self-defense. This would complicate Tokyo's ability to authorize a military response to a perceived Chinese escalation in the East China Sea, especially if such activity involves only Chinese maritime law enforcement—not naval—vessels.

Beijing has undertaken a number of steps since mid-2012 to address several shortcomings in its coordination of maritime policy to better align China's maritime activity with national policy. China's lack of a unified maritime strategy and multiple—sometimes overlapping—bureaucracies has previously been characterized as a model of inefficiency and an impediment to effective policy-making.⁶¹

In mid-2012, China created a new, high-level advisory group for maritime security issues. In China's foreign policy-making apparatus, key Chinese security policy issues, such as Taiwan, foreign affairs, and national security traditionally have merited their own high-level advisory groups within the Politburo Standing Committee.⁶² However, this is the first time maritime security has been elevated to this level, signaling the rising importance of this issue to Chinese leadership. The designation of Xi Jinping, who at the time was the top contender to be China's next senior leader, as the group's head, also indicates high-level attention to the matter. Furthermore, upon Japan's 2012 purchase of the Senkaku Islands, Beijing reportedly formed an "Office to Respond to the Diaoyu Crisis" and again placed Mr. Xi at the helm.⁶³

China previously had six chief maritime law enforcement agencies, all with separate and sometimes overlapping missions. In June 2013, China officially consolidated four of these six agencies—China Marine Surveillance, China Coast Guard, Fisheries Law Enforcement Command, and Maritime Customs Service—into the new China Coast Guard. The Maritime Safety Administration and China Rescue and Salvage remain independent.⁶⁴ The inaugural China Coast Guard patrol occurred near the Senkaku Islands, and was intended to "sternly declare the Chinese government's stance on its sovereignty over the Diaoyu Islands to Japanese vessels," according to an official Chinese statement.⁶⁵

While most of these ships previously had been unarmed, those subordinated to the China Coast Guard under the new structure could now be armed with mounted guns.⁶⁶ Furthermore, the China Coast Guard's capabilities will continue to modernize and improve in the next three to five years as it receives at least 30 new ocean-going ships and more than 100 smaller patrol boats. Most of these vessels will be larger and more capable than previous ones, and some will have the ability to embark helicopters. China's maritime law enforcement agencies also will continue to incorporate decommissioned ships from the PLA Navy into their own fleets—a practice that has increased in recent years.⁶⁷

Military Assertions of Maritime Sovereignty

The PLA Navy plays a powerful but indirect role in the East and South China Seas, backing up maritime law enforcement patrols from a distance; training, transiting, and conducting highly visible displays of presence in disputed waters; and resupplying Chinese-controlled islands in the South China Sea.*⁶⁸

- In March 2013, the PLA Navy sent a task force comprised of one large amphibious ship and three modern surface combatants to James Shoal, which is the southernmost point of China's maritime claim in the South China Sea and lies approximately 43 nm off the coast of Malaysia. According to official Chinese media, the crews of these vessels held a ceremony pledging to safeguard China's maritime interests upon reaching James Shoal. The task force then conducted training in the West Pacific before returning home.⁶⁹
- In May 2013, the PLA Navy conducted a rare, multifleet exercise involving elements of all three PLA Navy fleets in the South China Sea. While China's Ministry of National Defense described the exercise as "routine" and "not aimed at any specific country or target,"⁷⁰ some commentators suggested the exercise was used for political signaling during the China-Philippines standoff at Second Thomas Shoal and the transit of the U.S. Navy's *USS Nimitz* aircraft carrier through the region.⁷¹
- In mid-July 2013, following a joint exercise with the Russian Navy, a PLA Navy task force for the first time passed through the La Perouse Strait (also known as the Soya Strait), dividing northern Japan and Russia. The group of five vessels then transited east of Japan through the Pacific Ocean and back around southern Japan through the Miyako Strait dividing Japan's Miyako and Okinawa Islands, before reaching its homeport in Qingdao.⁷² Japanese press portrayed the route as "intended to demonstrate Chinese naval might to Japan and the United States and show Russia it means business in the region."⁷³ Official Chinese press heralded the event as a demonstration of the PLA Navy's ability to gain access to the Pacific Ocean through narrow chokepoints and to "cut the first island chain into several pieces," according to a PLA Navy official.⁷⁴ Chinese strategists and academics assert that the United States and Japan use the first island chain to strategically encircle or contain China and to prevent China from operating freely in the Pacific.[†]⁷⁵

The PLA Navy's regional power projection capability has advanced rapidly since the 1990s, boosting Beijing's ability to assert its maritime claims in the East and South China Seas and to respond forcefully to perceived challenges by rival claimants. See chapter 2, section 1, of this Report, "Military and Security Year in Review," for full coverage of China's naval modernization.⁷⁶

*U.S. Navy Seventh Fleet senior officers told the Commission PLA Navy vessels generally supported maritime law enforcement patrols at a distance of about 50 to 75 nm.

†The first island chain refers to the first chain of major archipelagoes east of the East Asian continent—from the Kuril Islands in the north, through the Japanese archipelago, Ryukyu Islands, Taiwan, the Philippines, and Borneo.

Risk of Unintended Escalation in the East and South China Seas

While Beijing's efforts to streamline its decision making on maritime disputes may reduce the risk of unintended escalation or accidents stemming from poor policy coordination, this risk is unlikely to be completely eliminated for the following reasons.

First, China's crisis management approach emphasizes demonstrating resolve to assert its sovereignty claims to rival claimants and domestic audiences. This characteristic, combined with China's tendency to view sovereignty in moralistic and absolutist terms, results in China's greater capacity to engage in escalatory actions in a foreign policy crisis.⁷⁷

Second, despite Beijing's efforts to consolidate its maritime bureaucracy, the fragmented nature of China's foreign policy structure could undermine Beijing's cohesiveness on maritime issues, particularly in the East China Sea. A major contributing factor is the limited authority of the Chinese Foreign Ministry. The Chinese Foreign Minister ranks several steps below the Politburo, whereas his Japanese counterpart occupies a much more influential position within the Japanese government. In some cases, this difference in protocol ranking between the two foreign ministries has prevented meaningful dialogue from taking place at the working level and could limit the capacity for crisis mitigation. For example, despite its limited authority, the Chinese Foreign Ministry was reportedly the only official channel open to Tokyo during the 2012 Senkaku Island crisis. Frequent turnover in Japanese leadership from 2006 to 2012 has further hindered the establishment of consistent official and unofficial diplomatic channels between the two countries.⁷⁸

The Ministry of Foreign Affairs in PRC Foreign Policymaking

Although China's Ministry of Foreign Affairs technically is responsible for the formulation and implementation of China's foreign policy, its influence has waned over the past decade. Due to China's increased political, economic, and military interaction with the world in recent decades, a wide array of actors has entered the Chinese foreign policymaking process through their direct dealings with foreign entities, including several national ministries, most provincial governments, the PLA, and state-owned firms.⁷⁹ As a result, the Ministry of Foreign Affairs is but one of several Chinese foreign policy actors that often have competing interests and goals. The exclusion of the foreign minister from China's 25-member Politburo since 1998 has further weakened the Ministry of Foreign Affairs' position in the foreign policymaking process. Though the opacity of the Chinese political system makes it difficult to render a definitive assessment, most analysts judge the Politburo and its seven-member Standing Committee make most of China's important foreign policy decisions.⁸⁰

For more information on the proliferation of official and non-official Chinese foreign policy actors, see chapter 3, section 2, of the Commission's 2011 Annual Report, "Actors in China's Foreign Policy."

Finally, deficiencies in civil-military coordination could continue to hamper policy coordination in the East and South China Seas. Officials at Japan's National Institute for Defense Studies, a policy think tank under the Japanese Ministry of Defense, told the Commission that coordination between the PLA and the Foreign Ministry, an important nexus in the management of China's maritime disputes, remains weak.⁸¹ The position of the PLA in the party bureaucracy outweighs and outranks the Foreign Ministry, which is one of many ministries under the State Council. Therefore, "for the Foreign Ministry to liaise with the PLA, it must report up to the State Council, which may have to report up further up to the Politburo in order to secure PLA cooperation," according to the Congressional Research Service.⁸² Such a structure does not lend itself to rapid or coordinated decision-making between the PLA and Foreign Ministry, which would be critical in a crisis in either the East or South China Seas.

The apparent maturation since the mid-2000s of China's National Committee on Border and Coastal Defense, an entity under the "dual leadership" of the State Council and the Central Military Commission that "coordinates China's border and coastal defense," suggests an effort to strengthen civil-military coordination with regard to border defense. However, outsiders know little about the influence of this organization on Beijing's overall management of the East and South China Sea disputes.⁸³

China's civil-military relationship also poses risks for crisis in the East and South China Seas at the operational level. Because the PLA routinely enjoys autonomy for military affairs, operational military activities that could significantly impact foreign affairs may not be approved at the highest levels before their execution.⁸⁴

For instance, on two occasions in late January 2013, a Chinese PLA Navy frigate reportedly locked weapons-targeting radar onto a Japan Maritime Self-Defense Force platform—first a helicopter, and later a destroyer. Public information on both Japanese and Chinese rules of engagement for ships and aircraft in the area is limited; however, illuminating another military asset with radar suggests hostile intent under international norms and increases the risk of miscalculation in an operational environment.⁸⁵

When queried about the incidents at a press conference, China's foreign ministry spokesperson stated the foreign ministry was "not aware of the matter" and knew of the incidents only through press reports.⁸⁶ Later in March, Japan's Kyodo News, citing unnamed high-level PLA officers, reported that the PLA admitted its frigates had locked its weapons-targeting radar onto the Japanese platforms. According to Kyodo, these PLA officers claimed the event, at least in the case of the destroyer, was reportedly due to an isolated "emergency decision" of the frigate's commander based on the Chinese military's rules of engagement.⁸⁷ China's Ministry of Defense dismissed the Kyodo report.⁸⁸ Nevertheless, the disconnect among Chinese entities in these cases suggests, as Rear Admiral McDevitt testified to the Commission, "that perhaps [the] ability [of Chinese leadership] to control the situation was not absolute."⁸⁹

Such close encounters are not limited to naval surface vessels. Japan also has reported an increasing number of Chinese aircraft within Japan's Air Defense Identification Zone. Between March

2012 and March 2013, the Japan Air Self-Defense Force scrambled fighter jets against Chinese aircraft in 306 instances—the largest number on record, and the first time this number surpassed the number of similar Japanese responses against Russia.⁹⁰ Furthermore, the Japanese Ministry of Defense in May 2013 reported three separate instances of PLA Navy submarine operations within Japan’s contiguous zone in the East China Sea, an UNCLOS-defined band of water that stretches from 12 to 24 nm from Japan’s coastal baselines.⁹¹ “Innocent passage” of submarines is lawful in contiguous zones and even in territorial waters, but the frequency and persistence of such operations at a time of ongoing tension was enough for Tokyo to raise the issue publically as a means to urge restraint.⁹²

These incidents, particularly the radar lock incident, “raise questions about . . . whether there’s an appreciation [in China] for the degree to which [these were] escalatory act[s],” as Roy Kamphausen, senior advisor for political and security affairs at the National Bureau for Asian Research, testified to the Commission.⁹³ As interactions between Chinese forces and U.S. and Japanese forces become more regular, the adherence of international protocols at sea will become increasingly important for the safety of all air and maritime operations in the region as well as the stability of the security situation in the East and South China Seas.

Implications for the United States

Beijing discourages and seeks to prevent the diplomatic involvement of the United States in the disputes, which Beijing considers a series of bilateral issues between China and each claimant. In response to interview questions on the role of the United States in the East China Sea, China’s Ambassador to the United States Cui Tiankai stated, “The most helpful thing the U.S. could do is to remain truly neutral, to take no side . . . When the United States talks to us, they say they’ll take no side, but sometimes, when they talk to the Japanese or when they make public statements, we hear something different.”⁹⁴

Although the United States does not take a position on the sovereignty of the disputed features and waters in the East and South China Seas, its treaty commitments bind it to the region in ways that link its security interests to the peaceful resolution of China’s maritime disputes.

In the East China Sea, the 1960 Treaty of Mutual Cooperation and Security between Japan and the United States of America provides for a U.S. commitment “in accordance with its constitutional provisions and processes” to defend Japan in the event of an armed attack “against either Party in the territories under the administration of Japan.”⁹⁵ The official U.S. position includes the Senkaku Islands, which are under Japanese administration, in its treaty obligations.⁹⁶ In the South China Sea, the United States maintains a treaty alliance with the Philippines based on the 1951 Mutual Defense Treaty between the United States and the Republic of the Philippines. Though the United States has affirmed its commitment to the Mutual Defense Treaty,⁹⁷ it has not officially articulated the specific geographic areas that would trigger a mutual de-

fense response to the Philippines. Some observers suggest this ambiguity regarding the Philippines' disputed land features has led Manila to misinterpret U.S. defense obligations, perhaps even emboldening Manila to challenge China.⁹⁸

Forward-deployed U.S. forces in East Asia are another element of U.S. security policy in the East and South China Seas. As Lt. Gen. Wallace "Chip" Gregson, USMC (Retd.), currently senior director for China and the Pacific at the Center for the National Interest, testified to the Commission, "Broad, active, widely distributed presence throughout the theater dampens sources of instability, deters conflict, gives substance to U.S. security commitments, and ensures continuing American access to the region."⁹⁹ As defense budgets tighten, the United States will face difficult choices in implementing its policy "rebalance" to Asia. A major challenge ahead for Washington, therefore, will be to stand firm on its security commitments while resourcing its overall foreign policy and security goals in the Asia Pacific region.¹⁰⁰ An integral part of this effort is evident in the deepening U.S. diplomatic and military engagement in the region, with an apparent emphasis on treaty alliances with the Philippines and Japan.¹⁰¹

Finally, the U.S.-China relationship is central to Washington's interest in the East and South China Sea disputes. Despite a generally improving military-to-military relationship, mutual mistrust about one another's long-term intentions continues to pervade the overall security relationship.¹⁰² This strategic backdrop poses challenges for the operational environment at sea, especially as the maritime operating areas of the two countries increasingly overlap. China's growing naval and maritime law enforcement advantage over its neighbors will add to already high levels of confidence that China can and should take bolder actions to protect its maritime interests. As U.S.-China air and naval interactions become more frequent, China's adherence to and participation in multilateral regimes regulating mariner interactions, such as the Convention on the International Regulations for Preventing Collisions at Sea and the Western Pacific Naval Symposium's Code of Unalerted Encounters at Sea, will become increasingly critical.¹⁰³

Through its diplomatic actions and the rebalance to Asia, the United States has signaled its intent to strengthen its relationship with partners and allies in East Asia. However, China's military modernization, coupled with the potential decline in U.S. power caused by sequestration, is altering the balance of power in the region and reducing the deterrent effect of the rebalance policy. The risk is therefore increasing that China's coercive approach to its sovereignty claims will lead to greater conflict in the region.

Conclusions

- China relies on a coercive and persistent maritime law enforcement and naval presence to gain control of disputed territory in the East and South China Seas. A consolidated maritime policy-making bureaucracy and streamlined maritime law enforcement fleets could increase Beijing's confidence in its capability for coercion in the ongoing maritime disputes.

- Two key drivers shape China's approach to its maritime disputes: First, China encourages ardent popular nationalism, which it exploits to support its foreign policy aims in the East and South China Seas. Second, China views sovereignty over claims in the East and South China Seas as central to its national security, territorial integrity, and economic development.
- China uses legal and administrative measures to assert de jure governance over its disputed maritime regions; it deploys maritime law enforcement and naval vessels to its claimed waters to demonstrate and lay the groundwork for de facto governance.
- Beijing's tendency to demonstrate resolve in its maritime disputes; its large and complicated political, foreign affairs, and military bureaucracy; and its inconsistent adherence to internationally accepted norms of air and maritime operations may contribute to operational miscalculations in the East and South China Seas. Unyielding positions on sovereignty and nationalist sentiment surrounding these maritime disputes increase the risk of escalation from a miscalculation at sea to a political crisis.

ENDNOTES FOR SECTION 3

1. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Peter Dutton, April 4, 2013.
2. Ministry of Foreign Affairs (Taiwan), "The Diaoyutai Islands: An Inherent Part of the Territory of the Republic of China (Taiwan)," (Taipei, Taiwan: April 2012). <http://www.mofa.gov.tw/official/Home/Detail/4ad52054-ebc7-452c-a6c1-d182b25c8001?arfid=2b7802ba-d5e8-4538-9ec2-4eb818179015&opno=027ffe58-09dd-4b7c-a554-99def06b00a1>; State Council Information Office (China), *Diaoyu Dao, an Inherent Territory of China* (Beijing, China: State Council, September 2012). http://www.china.org.cn/government/whitepaper/2012-09/25/content_26628166.htm.
3. Mark E. Manyin, *Senkaku (Diaoyu/Diaoyutai) Islands Dispute: U.S. Treaty Obligations* (Washington, DC, Congressional Research Service: January 2013), pp. 4–5; Paul J. Smith, "The Senkaku/Diaoyu Island Controversy: A Crisis Postponed," *Japan's Territorial Disputes: CNA Maritime Asia Project: Workshop Three* (Alexandria, VA: CNA: June 2013) pp. 129–139. <http://www.cna.org/sites/default/files/research/JapansTerritorialDisputes.pdf>.
4. Michael A. McDevitt and Catherine K. Lea, "Workshop Overview," *Japan's Territorial Disputes: CNA Maritime Asia Project: Workshop Three* (Alexandria, VA: CNA: June 2013) p. 5. <http://www.cna.org/sites/default/files/research/JapansTerritorialDisputes.pdf>; Ministry of Foreign Affairs (Japan), "The Basic View on the Sovereignty over the Senkaku Islands" (Tokyo, Japan: May 2013), http://www.mofa.go.jp/region/asia-pacific/senkaku/basic_view.html.
5. Kyodo, "U.S. warned government against buying Senkaku Islands: Campbell," April 10, 2013. <http://www.japantimes.co.jp/news/2013/04/10/national/u-s-warned-government-against-buying-senkaku-islands-campbell/#.Uk7CilCsiSo>.
6. State Council Information Office (China), "Foreword," in *Diaoyu Dao, an Inherent Territory of China* (Beijing, China: State Council, September 2012). http://www.china.org.cn/government/whitepaper/2012-09/25/content_26628166.htm.
7. UN Convention on the Law of the Sea, Part V: Exclusive Economic Zone, "Article 56: Rights, jurisdiction, and duties of the coastal State in the exclusive economic zone." http://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm.
8. UN Convention on the Law of the Sea, Part V: Exclusive Economic Zone, "Article 76: Definition of the continental shelf." http://www.un.org/depts/los/convention_agreements/texts/unclos/part6.htm; UN Convention on the Law of the Sea, Part V: Exclusive Economic Zone, "Article 77: Rights of the coastal State over the continental shelf." http://www.un.org/depts/los/convention_agreements/texts/unclos/part6.htm.
9. Ben Dolven, Shirley A. Kan, and Mark E. Manyin, *Maritime Territorial Disputes in East Asia: Issues for Congress* (Washington, DC: Congressional Research Service, January 2013), p. 13; Xinjun Zhang, *China's "Peaceful Rise," "Harmonious" Foreign Relations, and Legal Confrontation—and Lessons from the Sino-Japanese Dispute over the East China Sea* (Philadelphia, PA: Foreign Policy Research Institute, April 2010). <http://www.fpri.org/enotes/201004.zhang.chinariselegalconfrontation.html>; and People's Republic of China, "Executive Summary—Submission by the People's Republic of China Concerning the Outer Limits of the Continental Shelf beyond 200 Nautical Miles in Part of the East China Sea," December 14, 2012. http://www.un.org/depts/los/clcs_new/submissions_files/chn63_12/executive%20summary_EN.pdf.
10. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, testimony of Michael McDevitt, April 4, 2013.
11. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Michael Swaine, April 4, 2013.
12. Bonnie S. Glaser and Leon Zhihong Bai, "Chinese Perspectives on the Senkaku/Diaoyu Islands Dispute," *Japan's Territorial Disputes: CNA Maritime Asia Project: Workshop Three* (Alexandria, VA: CNA, June 2013), pp. 93–94. <http://www.cna.org/sites/default/files/research/JapansTerritorialDisputes.pdf>; M. Taylor Fravel, "Drawing Lines in the Water," *Diplomat*, September 14, 2012. <http://thediplomat.com/china-power/drawing-lines-in-the-water/>.
13. M. Taylor Fravel, "Xi Jinping's Overlooked Revelation on China's Maritime Disputes," *Diplomat*, August 15, 2013. <http://thediplomat.com/2013/08/15/xi-jinpings-overlooked-revelation-on-chinas-maritime-disputes/?all=true>; Xinhua, "Xi Jinping Stresses the Need to Show Greater Care about the Ocean, Understand More about the Ocean, and Make Strategic Plans for the Use of the Ocean, Push Forward the

Building of a Maritime Power and Continuously Make New Achievements at the Eighth Collective Study Session of the CPC Central Committee Political Bureau,” July 31, 2013. OSC ID: CHR2013073144047122. <http://www.opensource.gov>.

14. Zheng Wang, “Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations,” *Montreal Review*, November 2012. <http://www.themontrealreview.com/2009/Never-Forget-National-Humiliation-Historical-Memory-in-Chinese-Politics-and-Foreign-Relations.php>; “Interview with Zheng Wang, Author of *Never Forget National Humiliation: Historical Memory in Chinese Politics and Foreign Relations*” (New York, NY: Columbia University Press, 2012). <http://www.cup.columbia.edu/static/zheng-wang-interview>.

15. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, testimony of Jessica Chen Weiss, April 4, 2013.

16. Barbara Demick, “China video of man beaten in anti-Japan riot spurs soul searching,” *Los Angeles Times*, September 27, 2012. <http://articles.latimes.com/2012/sep/27/world/la-fg-china-japan-cars-20120927>; Gordon G. Chang, “Is China Burning?” *Forbes*, September 23, 2012. <http://www.forbes.com/sites/gordonchang/2012/09/23/is-china-burning/>.

17. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Jessica Chen Weiss, April 4, 2013.

18. Atsushi Okudera, “Chinese Coast Guard prevents private Chinese yacht from visiting Senkaku Islands,” *Asahi Shimbun* (Tokyo), August 10, 2013. http://ajw.asahi.com/article/behind_news/social_affairs/AJ201308100052; Yuka Hayashi, “China, Japan Show Restraint Ahead of WWII Anniversary,” *Wall Street Journal: Japan Real Time*, August 14, 2013. <http://blogs.wsj.com/japanrealttime/2013/08/14/china-japan-show-restraint-ahead-of-wwii-anniversary/>.

19. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Jessica Chen Weiss, April 4, 2013.

20. Michael D. Swaine, “Chinese Views Regarding the Senkaku/Diaoyu Islands Dispute,” *China Leadership Monitor* 41 (June 6, 2013), p. 3. <http://www.hoover.org/publications/china-leadership-monitor/article/148786>; State Council Information Office (China), *Diaoyu Dao, an Inherent Territory of China* (Beijing, China: September 2012). http://www.china.org.cn/government/whitepaper/2012-09/25/content_26628166.htm.

21. Hillary Clinton et al., “Closing Remarks for U.S.-China Security and Economic Dialogue” (Eisenhower Executive Office Building, Washington, DC, July 28, 2009). <http://www.state.gov/secretary/rm/2009a/july/126599.htm>; Michael Swaine, “China’s Assertive Behavior: Part One: On ‘Core Interests,’” *China Leadership Monitor* 34 (February 22, 2011), p. 4. <http://www.hoover.org/publications/china-leadership-monitor/article/67966>; and Stephanie Kleine-Ahlbrandt (contributor), “Does Promoting ‘Core Interests’ Do China More Harm than Good?” *ChinaFile Conversation*, May 2, 2013. <http://www.chinafile.com/does-promoting-core-interests-do-china-more-harm-good>.

22. Permanent Mission of the People’s Republic of China to the United Nations Office at Geneva and other International Organizations in Switzerland, “Foreign Ministry Spokesman Qin Gang’s Regular Press Conference on November 27, 2008,” November 28, 2008. <http://www.china-un.ch/eng/fyrth/t524172.htm>; Xinhua, “Tang Jiaquan Meets U.S. Secretary of State” (translation), January 20, 2003. http://news.xinhuanet.com/zhengfu/2003-01/20/content_697563.htm; Ministry of Foreign Affairs (China), “Foreign Ministry spokesperson Kong Quan warns the U.S. for its decision to sell Taiwan the long-range radar system and answers a reporter’s question” (translation), January 1, 2004. http://www.fmprc.gov.cn/mfa_chn/wjdt_611265/fyrbt_611275/t82122.shtml; and Michael Swaine, “China’s Assertive Behavior: Part One: On ‘Core Interests,’” *China Leadership Monitor* 34 (February 22, 2011): 8. <http://www.hoover.org/publications/china-leadership-monitor/article/67966>.

23. Edward Wong, “Chinese Military Seeks to Extend Its Naval Power,” *New York Times*, April 23, 2010. <http://www.nytimes.com/2010/04/24/world/asia/24navy.html?pagewanted=all>; Michael Swaine, “China’s Assertive Behavior: Part One: On ‘Core Interests,’” *China Leadership Monitor* 34 (February 22, 2011): 9, 23. <http://www.hoover.org/publications/china-leadership-monitor/article/67966>; and Alastair Iain Johnston, “How New and Assertive is China’s New Assertiveness?” *International Security* 34:7 (Spring 2013): 17–18.

24. Kyodo, “China Says Senkaku Islands are its ‘Core Interest,’” April 26, 2013. OSC ID: JPP20130426969071. <http://www.opensource.gov>; *Asahi Shimbun* (Tokyo), “Japanese, Chinese Defense Officials Meet to Ease Tensions Over Senkakus,” April 27, 2013. <http://ajw.asahi.com/article/asia/china/AJ201304270049>.

25. Caitlin Campbell et al., *China's 'Core Interests' and the East China Sea* (Washington, DC: U.S.-China Economic and Security Review Commission, May 2013), p. 5. <http://www.uscc.gov/Research/china%E2%80%99s-%E2%80%9Ccore-interests%E2%80%9D-and-east-china-sea>.

26. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Lloyd Thrall, April 4, 2013.

27. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Lloyd Thrall, April 4, 2013.

28. Chris Acheson, "An Interview with James Manicom: Disputed Claims in the East China Sea" (Seattle, WA: National Bureau of Asian Research, July 25, 2011). <http://www.nbr.org/research/activity.aspx?id=159#UcsT5Pn2boI>; Nick Owen, "Oil Disputes in the South China Sea in Context," in *Maritime Energy Resources in Asia: Energy and Geopolitics* (Seattle, WA: National Bureau of Asian Research, 2011), pp. 11–38.

29. David Rosenberg, "The Paradox of South China Sea Disputes," *The China Story* (Canberra), April 23, 2013. <http://www.thechinastory.org/2013/04/the-paradox-of-the-south-china-sea-disputes/>.

30. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Steven Rice, April 4, 2013.

31. U.S. Energy Information Administration, *South China Sea* (Washington, DC: February 2013). <http://www.eia.gov/countries/regions-topics.cfm?fips=SCS>.

32. U.S. Energy Information Administration, *South China Sea* (Washington, DC: February 2013). <http://www.eia.gov/countries/regions-topics.cfm?fips=SCS>; U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Steven Rice, April 4, 2013.

33. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Lloyd Thrall, April 4, 2013.

34. *Taiwan Today*, "Taiwan lifts sanctions against Philippines," August 9, 2013. <http://taiwantoday.tw/ct.asp?xItem=208324&ctNode=1983>.

35. Xinhua, "South China Sea issue should be resolved through negotiations by parties directly concerned," July 2, 2013. OSC ID: CPP20130702786001. <http://www.opensource.gov>.

36. "Declaration on the Conduct of Parties in the South China Sea," November 4, 2002. <http://www.asean.org/asean/external-relations/china/item/declaration-on-the-conduct-of-parties-in-the-south-china-sea>; Xinjun Zhang, *The South China Sea Issue and the Role of International Law: a Chinese Perspective* (Washington, DC: Center for Strategic and International Studies, June 5–6, 2013), p. 3. http://csis.org/files/attachments/130606_Zhang_ConferencePaper.pdf.

37. Xinhua, "Wang Yi Comments on the Process of Pushing Forward the 'Code of Conduct in the South China Sea,'" August 5, 2013. OSC ID: CHR2013080519663440. <http://www.opensource.gov>; Joanna Chiu, "Beijing tells Asean to be realistic in hopes for South China Sea code of conduct," *South China Morning Post* (Hong Kong), August 6, 2013. <http://www.scmp.com/news/china/article/1294453/foreign-minister-wang-yi-says-china-no-hurry-sign-south-china-sea-accord>.

38. Ministry of Foreign Affairs (China), "Foreign Ministry Spokesperson Hua Chunying's Remarks on the Philippines' Efforts in Pushing for the Establishment of the Arbitral Tribunal in Relation to the Disputes between China and the Philippines in the South China Sea" (Beijing, China: April 26, 2013). <http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t1035577.shtml>.

39. Ministry of Foreign Affairs (China), "Foreign Ministry Spokesperson Hua Chunying's Remarks on the Philippines' Efforts in Pushing for the Establishment of the Arbitral Tribunal in Relation to the Disputes between China and the Philippines in the South China Sea" (Beijing, China: April 26, 2013). <http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t1035577.shtml>.

40. Permanent Court of Arbitration, "Arbitration between the Republic of the Philippines and the People's Republic of China," August 27, 2013. http://www.pca-cpa.org/showpage.asp?pag_id=1529; Mark Valencia, "Political maelstrom gathers force in the South China Sea," *Straits Times* (Singapore), August 10, 2013. <http://www.straitstimes.com/the-big-story/asia-report/china/story/political-maelstrom-gathers-force-south-china-sea-20130810>; and Ministry of Foreign Affairs (Philippines), "Statement by Secretary of Foreign Affairs Albert del Rosario on the UNCLOS Arbitral Proceedings against China to Achieve a Peaceful and Durable Solution to the Dispute in the WPS," January 22, 2013. <http://www.philippineembassy-usa.org/news/3071/300/Statement-by-Secretary-of-Foreign-Affairs-Albert-del-Rosario-on-the->

UNCLOS-Arbitral-Proceedings-against-China-to-Achieve-a-Peaceful-and-Durable-Solution-to-the-Dispute-in-the-WPS/d,phildet/; and Paul Reichler (Partner, Foley Hoag), e-mail interview with Commission staff.

41. Henry Bensurto, *Role of International Law in Managing Disputes in the South China Sea* (Washington, DC: Center for Strategic and International Studies, June 5–6, 2013). http://csis.org/files/attachments/130606_Bensurto_ConferencePaper.pdf; Rosemarie Francisco and Manuel Mogato, “Philippines says China expanding territory before code takes effect,” Reuters, September 4, 2013. <http://www.reuters.com/article/2013/09/04/us-philippines-china-idUSBRE9830KQ20130904>; and T.J. Burgonio and Jaymee T. Gamil, “China Row on Agenda of Bolkia-Aquino Talks,” *Philippine Daily Inquirer*, April 16, 2013. OSC ID: SEP20130416007001. <http://www.opensource.gov>.

42. Zhong Sheng, “How Can Hying on the Code of Conduct Be Tolerated,” *People’s Daily*, August 12, 2013. OSC ID: CHO2013081220931316. <http://www.opensource.gov>.

43. People’s Republic of China, “Statement of the Government of the People’s Republic of China On the Baselines of the Territorial Sea of Diaoyu Dao and Its Affiliated Islands,” September 10, 2012. http://www.un.org/Depts/los/LEGISLATIONANDTREATIES/PDFFILES/DEPOSIT/chn_mzn89_2012_e.pdf.

44. Permanent Mission of Japan to the United Nations, correspondence with the Secretary-General of the United Nations, September 24, 2012. http://www.un.org/Depts/los/LEGISLATIONANDTREATIES/PDFFILES/DEPOSIT/communications_redeposit/mzn89_2012_jpn.pdf.

45. U.S. Department of Defense, *Maritime Claims Reference Manual* (Washington, DC: 2013). <http://www.jag.navy.mil/organization/documents/mcrm/China2013.pdf>; U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: May 2013), p. 4. http://www.defense.gov/pubs/2013_china_report_final.pdf.

46. Malcolm Moore, “China’s neighbours protest its passport map grab,” *Telegraph* (London), November 2, 2012. <http://www.telegraph.co.uk/news/worldnews/asia/china/9695732/Chinas-neighbours-protest-its-passport-map-grab.html>; Agence France-Presse, “US to raise passports row with China, calling it ‘unhelpful,’” August 29, 2013. <http://www.scmp.com/news/china/article/1092764/us-raise-passports-row-china-calling-it-unhelpful>.

47. M. Taylor Fravel, “Hainan’s New Maritime Regulations: An Update,” *Diplomat*, January 4, 2013. <http://thediplomat.com/china-power/hainans-new-maritime-regulations-an-update/>; Ben Blanchard and Manuel Mogato, “UPDATE 4—Chinese police plan to board vessels in disputed seas,” Reuters, November 29, 2012. <http://www.reuters.com/article/2012/11/30/china-seas-idUSL4N0991Z020121130>.

48. Jeremy Page, “China Sheds Light on New Sea Rules,” *Wall Street Journal*, December 5, 2012. <http://online.wsj.com/article/SB10001424127887323717004578158992804807854.html>.

49. Carlyle A. Thayer, “China’s New 10-Dash Line Claim to the South China Sea,” Thayer Consultancy Background Brief, July 18, 2013; Peter Dutton, “Three Disputes and Three Objectives,” *U.S. Naval War College Review* 64:4 (Autumn 2011): 64. <http://www.usnwc.edu/getattachment/feb516bf-9d93-4d5c-80dc-d5073ad84d9b/Three-Disputes-and-Three-Objectives—China-and-the>; and Euan Graham, “China’s new map: just another dash?” *The Strategist: Australian Strategic Policy Institute Blog*, September 17, 2013. <http://www.aspistrategist.org.au/chinas-new-map-just-another-dash/>.

50. Xinhua Digest, “Xinban Zhongguo ditu yang lie Nanhai zhudao he Diaoyu dao, Zhuzhong xuanshi zhuquan” (New edition of China territory map depicts South China Sea islands and Diaoyu islands, Lays emphasis on the proclamation of sovereign rights), January 13, 2013. <http://world.people.com.cn/n/2013/0113/c157278-20182571.html>; Jiang Yan, “No More Downscaling for South China Sea Islands—Map Press Puts Out Vertical maps of China, Showing South China Sea Islands and Mainland on the Same Scale for the First Time,” *Xinjing Bao* (Beijing News), January 7, 2013. OSC ID: CPP20130116047001. <http://www.opensource.gov>.

51. U.S.-China Economic and Security Review, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), p. 215.

52. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Michael McDevitt, April 4, 2013; U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Michael Swaine, April 4, 2013; and U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Peter Dutton, April 4, 2013.

53. M. Taylor Fravel, "China's Island Strategy: 'Redefining the Status Quo,'" *Diplomat*, November 1, 2012. <http://thediplomat.com/china-power/chinas-island-strategy-redefine-the-status-quo/>.

54. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Michael McDevitt, April 4, 2013; International Crisis Group, *Dangerous Waters: China-Japan Relations on the Rocks* (Brussels, Belgium: April 2013), pp. 12–15. <http://www.crisisgroup.org/-/media/Files/asia/north-east-asia/245-dangerous-waters-china-japan-relations-on-the-rocks.pdf>.

55. U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2012), p. 232.

56. Mario J. Mallari, "Scarborough Remains under AFP Monitoring as Long as it Takes," *Daily Tribune* (Manila), September 5, 2013. OSC ID: SEO2013090523117716. <http://www.opensource.gov>; Carlyle Thayer, "To Isolate Philippines, China Woos ASEAN," *Diplomat*, October 1, 2013. <http://thediplomat.com/flashpoints-blog/2013/10/01/to-isolate-philippines-china-woos-asean/>.

57. Manuel Mogato, "South China Sea tension mounts near Filipino shipwreck," Reuters, May 28, 2013. <http://www.reuters.com/article/2013/05/28/us-philippines-china-idUSBRE94R0YS20130528>; Victor Reyes, "China Ships Still at Shoal: But 30 Fishing Vessels Are Gone," *Malaya Business Insight* (Manila), May 27, 2013. OSC ID: SEP20130527007003. <http://www.opensource.gov>; Ellen Tordesillas, "China Offers to Remove 'Sierra Madre' From Ayungin Shoal," *Malaya Business Insight* (Manila), July 3, 2013. OSC ID: SEO2013070337521909. <http://www.opensource.gov>; Cecil Morella, "Grounded ship is Philippines' last line of defence against China," *Agence France-Presse*, May 26, 2013. <http://www.taipetimes.com/News/editorials/archives/2013/05/26/2003563187/2>; and NavSource Naval History, "USS Harnett County (AGP-821)," April 19, 2013. <http://www.navsource.org/archives/10/16/160821.htm>.

58. Ministry of Foreign Affairs (China), "Transcript of PRC FM Spokesman News Conference 24 June 13, hosted by Hua Chunying," OSC ID: CPP20130624364001. <http://www.opensource.gov>; Ministry of Foreign Affairs (China), "Transcript of PRC FM Spokesman News Conference 30 May 13, hosted by Hong Lei," OSC ID: CPP20130530364001. <http://www.opensource.gov>.

59. Open Source Center, "Increase in Reported PRC Military Activity Near Senkaku Islands Suggests Beijing Hardening Stance," May 3, 2013. OSC ID: JPF20130503215002. <http://www.opensource.gov>; State Oceanic Administration (China) "Diaoyu dao weichuan xunhang Yi zhou nian huigu" (Diaoyu Islands Rights Protection Patrols—a one year retrospective), September 10, 2013. http://www.soa.gov.cn/xw/ztd/2012/dydszgdssl/dydszgdssl_549/201309/t20130910_27288.htm.

60. John W. Traphagan, "Revising the Japanese Constitution," *Diplomat*, May 17, 2013. <http://thediplomat.com/the-editor/2013/05/17/revising-the-japanese-constitution/>; Aureila George Mulgan, "Abe rocks Japan's constitutional boat," *East Asia Forum*, May 21, 2013. <http://www.eastasiaforum.org/2013/05/21/abe-rocks-japans-constitutional-boat/>; and Yuka Hayashi, "Japan Leader Charts Path for Military Rise," *Wall Street Journal*, April 24, 2013. <http://online.wsj.com/article/SB10001424127887323551004578438253084917008.html>.

61. International Crisis Group, *Stirring Up the South China Sea (I)*, (Brussels, Belgium: April 2012), pp. 14–26. <http://www.crisisgroup.org/-/media/Files/asia/north-east-asia/223-stirring-up-the-south-china-sea-i.pdf>.

62. Alice Miller, "The CCP Central Committee's Leading Small Groups," *China Leadership Monitor* 26 (Fall 2008): 3. <http://media.hoover.org/sites/default/files/documents/CLM26AM.pdf>.

63. Linda Jakobson, "How Involved is Xi Jinping in the Diaoyu Crisis?" *Diplomat*, February 8, 2013. <http://thediplomat.com/2013/02/08/how-involved-is-xi-jinping-in-the-diaoyu-crisis-3/>; Linda Jakobson, *China's Foreign Policy Dilemma* (Sydney, Australia: Lowy Institute for International Policy, February 2013), p. 9; and *Sydney Morning Herald*, "Fresh South China Sea dispute," December 5, 2012. <http://www.smh.com.au/world/fresh-south-china-sea-dispute-20121205-2aupd.html>.

64. General Office of the State Council (China), "Guowuyuan bangongting guanyu yinfa guojia haiyangju zhuyao zhize nei she jigou he renyuan bianzhi guiding de tongzhi" (Notice of the General Office of the State Council on Issuing Provisions on the Main Duties, Internal Organization, and Personnel Organization of the State Oceanic Administration), June 9, 2013 (Beijing, China). http://www.gov.cn/zwgh/2013-07/09/content_2443023.htm; U.S. Office of Naval Intelligence, Regional Maritime Law Enforcement Overview, written response to request for information provided to the U.S.-China Economic and Security Review Commission (Suitland, MD: June 24, 2013); Jin Chang and Zhu Yu, "State Council Plans to Reorganize SOA, Set Up National Oceanic Commission; SOA to Protect Sovereignty, Enforce

Laws in Name of PRC Coast Guard,” *Zhongguo Haiyang Bao* (China Maritime News), March 12, 2013. OSC ID: CPP20130312680007. <http://www.opensource.gov>; and Craig Murray et al., *China’s Naval Modernization and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, August 2013). <http://www.uscc.gov/Research/china%E2%80%99s-naval-modernization-and-implications-united-states>.

65. State Oceanic Administration (China), “China Coast Guard Formation Declares Sovereignty in Diaoyu Sea Area,” July 26, 2013. OSC ID: CHR2013072646375311. <http://www.opensource.gov>.

66. Jane Perlez, “China, With Revamped Force, Makes Presence Known in East China Sea,” *New York Times*, July 27, 2013. <http://www.nytimes.com/2013/07/28/world/asia/chinese-with-revamped-force-make-presence-known-in-east-china-sea.html>.

67. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: May 2013), p. 40; Jane Perlez, “Chinese, With Revamped Force, Make Presence Known in South China Sea,” *New York Times*, July 27, 2013. http://www.nytimes.com/2013/07/28/world/asia/chinese-with-revamped-force-make-presence-known-in-east-china-sea.html?_r=0; and Craig Murray et al., *China’s Naval Modernization and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, August 2013). <http://www.uscc.gov/Research/china%E2%80%99s-naval-modernization-and-implications-united-states>.

68. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Michael McDevitt; U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, November 2012), p. 215; and U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, testimony of Peter Dutton, April 4, 2013.

69. Bai Ruixue, Gao Yi, and Gan Jun, “(Military) From South China Sea to West Pacific: Complete Record of Navy Task Force’s Distant Sea Training of Combat-Readiness Patrol,” *Xinhua*, April 3, 2013. OSC ID: CPP20130403072005. <http://www.opensource.gov>; Jeremy Page, “Chinese Ships Approach Malaysia,” *Wall Street Journal*, March 27, 2013. <http://online.wsj.com/article/SB10001424127887324685104578386052690151508.html>; and Zhao Lei, “Combatant ships patrol the South China Sea,” *China Daily*, March 27, 2013. http://www.chinadaily.com.cn/china/2013-03/27/content_16350358.htm.

70. Ministry of National Defense (China), “Transcript of PRC National Defense Ministry’s News Conference 30 May 2013” (Beijing, China: May 30, 2013). OSC ID: CPP20130601355001. <http://www.opensource.gov>.

71. Choi Chi-yuk, “PLA Navy’s three fleets meet in South China Sea for a rare show of force,” *South China Morning Post* (Hong Kong), May 27, 2013. <http://www.scmp.com/news/china/article/1246897/pla-navys-three-fleets-meet-south-china-sea-rare-show-force>; *Want China Times* (Taipei), “3 PLA fleets complete major exercise in South China Sea,” May 27, 2013. <http://www.wantchinatimes.com/news-subclass-ent.aspx?id=20130527000045&cid=1101>.

72. Jonathan Soble and Leslie Hook, “Chinese warships sail past northern Japan,” *Financial Times* (London), July 14, 2013. <http://www.ft.com/intl/cms/s/0/8673fa70-ec5b-11e2-8096-00144feabdc0.html?siteedition=intl#axzz2Z9hgZcIH>.

73. *Asahi Shimbun* (Tokyo), “Chinese warships make circuit of Japanese archipelago,” July 23, 2013. <http://ajw.asahi.com/article/asia/china/AJ201307230082>.

74. Li Xiaokun, “China sails through ‘first island chain,’” *China Daily*, August 2, 2013. http://usa.chinadaily.com.cn/china/2013-08/02/content_16863855.htm.

75. Fu Xianming, “The United States Is Quietly Building New-Generation Overseas Military Bases. They Are Just Like Lily Pads in a Pond, Which Are Small but Allow Frogs To Use Them To Jump Around and Prey at Will. As the Obama Administration Is Shifting its Global Strategy to Asia, the Pentagon Is Trying to Make the ‘Water Lilies’ Blossom All Over the Entire Asia-Pacific Region—‘Water Lilies’ of US Armed Forces Lie Low in Asia-Pacific,” *Chengdu Zhanqi Bao* (Chengdu Front News), February 6, 2013. OSC ID: CPP20130520503003. <http://www.opensource.gov>.

76. Craig Murray et al., *China’s Naval Modernization and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, August 2013). <http://www.uscc.gov/Research/china%E2%80%99s-naval-modernization-and-implications-united-states>.

77. U.S.-China Economic and Security Review Commission, *Hearing on China’s Maritime Disputes in the East and South China Seas*, written testimony of Michael Swaine, April 4, 2013.

78. International Crisis Group, *Dangerous Waters: China-Japan Relations on the Rocks* (Brussels, Belgium: April 2013), pp. 28–35. <http://www.crisisgroup.org/>

media/Files/asia/north-east-asia/245-dangerous-waters-china-japan-relations-on-the-rocks.pdf.

79. Yufan Hao, "Domestic Chinese Influences on US-China Relations," in David Shambaugh, ed., *Tangled Titans* (New York: Rowman and Littlefield, 2012), p. 127.

80. Linda Jakobson and Dean Knox, *New Foreign Policy Actors in China* (Stockholm, Sweden: Stockholm International Peace Research Institute, September 2010), p. 4. <http://books.sipri.org/files/PP/SIPRIIPP26.pdf>.

81. See also Ministry of National Defense (Japan), *China Security Report 2012* (Tokyo, Japan: National Institute for Defense Studies, December 2012) pp. 28–30. http://www.nids.go.jp/publication/chinareport/pdf/china_report_EN_web_2012_A01.pdf; Susan V. Lawrence and Michael F. Martin, *Understanding China's Political System* (Washington, DC: Congressional Research Service, March 2013) <http://www.fas.org/sgp/crs/row/R41007.pdf>; and Michael D. Swaine, "China's Assertive Behavior: Part Three: The Role of the Military in Foreign Policy," *China Leadership Monitor* 36 (Winter 2012). <http://media.hoover.org/sites/default/files/documents/CLM36MS.pdf>.

82. Susan V. Lawrence and Michael F. Martin, *Understanding China's Political System* (Washington, DC: Congressional Research Service, March 2013), p. 15. <http://www.fas.org/sgp/crs/row/R41007.pdf>.

83. State Council Information Office (China), *China's National Defense in 2006* (Beijing, China: December 2006). <http://www.china.org.cn/english/features/book/194421.htm>; State Council Information Office (China), *China's National Defense in 2010* (Beijing, China: March 2011). http://www.china.org.cn/government/whitepaper/node_7114675.htm; and National Institute for Defense Studies (Japan), *China Security Report 2012* (Tokyo, Japan: 2012), pp. 34–35. http://www.nids.go.jp/publication/chinareport/pdf/china_report_EN_web_2012_A01.pdf.

84. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, testimony of Roy Kamphausen, February 7, 2013; Michael D. Swaine, "China's Assertive Behavior: Part Three: The Role of the Military in Foreign Policy," *China Leadership Monitor* 36 (Winter 2012), pp. 3–4. <http://media.hoover.org/sites/default/files/documents/CLM36MS.pdf>.

85. Dennis Mandsager et al., *Rules of Engagement Handbook* (San Remo, Italy: International Institute of Humanitarian Law, November 2009), pp. 22–23; Itsunori Onodera, "Extra Press Conference by the Defense Minister" (Tokyo, Japan: Ministry of Defense, February 5, 2013). <http://www.mod.go.jp/e/pressconf/2013/02/130205a.html>.

86. John Brinsley and Isabel Reynolds, "Abe Calls China Radar Targeting of Japan Vessel Provocative," Bloomberg, February 6, 2013. <http://www.bloomberg.com/news/2013-02-05/china-targeted-japanese-naval-vessel-with-radar-nhk-reports.html>.

87. Kyodo, "Chinese officials admit to MSDF [Maritime Self Defense Force] radar lock allegations," March 18, 2013. <http://www.japantimes.co.jp/news/2013/03/18/national/chinese-officials-admit-to-msdf-radar-lock-allegations/#.Ue1JjndGXmk>; Samuel Wade, "Chinese Officials Said to Admit Radar Lock (Updated)," *China Digital Times*, March 18, 2013. <http://chinadigitaltimes.net/2013/03/chinese-officials-said-to-admit-radar-lock-incident/>; and Satoshi Tomizaka, "Who is Responsible for PLAN Radar Lock-On Incident?" *Shukan Bunshun* (Tokyo), February 21, 2013. English translation at: <http://jsw.newpacificinstitute.org/?p=10876>.

88. Zhang Yunbi, "Beijing dismisses Japan's 'radar lock' media report," *China Daily*, March 19, 2013. <http://english.peopledaily.com.cn/90883/8173056.html>.

89. U.S.-China Economic and Security Review Commission, *Hearing on China's Maritime Disputes in the East and South China Seas*, written testimony of Michael McDevitt, April 4, 2013.

90. Ministry of Defense (Japan), "Japan Details Scramble Mission Against PRC, Russian Aircraft Apr 2012—Mar 2013" (Tokyo, Japan). OSC ID: JPP20130418014001. <http://www.opensource.gov>; *Asahi Shimbun* (Tokyo), "INSIGHT: China puts Japan on notice that its scrambles are now routine," July 30, 2013. http://ajw.asahi.com/article/behind_news/politics/AJ201307300099.

91. Alexander Martin, "Japan on Alert Over Unidentified Submarines," *Wall Street Journal*, May 14, 2013. <http://online.wsj.com/article/SB10001424127887323716304578482331157168110.html>; *Sankei Shimbun* (Tokyo), "Defense Ministry Concludes Latest Chinese Yuan-Class Submarines Were Sailing in Contiguous Zones; Japanese, US Ocean Surveillance Ships Deployed To Detect Subs," May 26, 2013. OSC ID: JPP20130526033005. <http://www.opensource.gov>.

92. *Japan News* (Tokyo), "Sound Waves Used Against 'Chinese' Sub," May 21, 2013. OSC ID: JPP20130521969092. <http://www.opensource.gov>; *Asahi Shimbun* (Tokyo), "Move to publicize submarine locations proves ineffective," May 21, 2013. http://ajw.asahi.com/article/behind_news/politics/AJ201305210052; Peter A. Dutton, "International Law and the November 2004 'Han Incident'," in Andrew S. Erickson

et al., *China's Future Nuclear Submarine Force* (Annapolis, MD: U.S. Naval Institute, 2007), pp. 163–169.; UN Convention on the Law of the Sea, Part II: Territorial Sea and Contiguous Zone, “Article 19: Meaning of innocent passage,” http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm; and UN Convention on the Law of the Sea, Part II: Territorial Sea and Contiguous Zone, “Article 20: Submarines and other underwater vehicles,” http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm.

93. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, testimony of Roy Kamphausen, February 7, 2013.

94. Jonathan Tepperman, “Beijing’s Brand Ambassador: A Conversation with Cui Tiankai,” *Foreign Affairs* 92:4 (July/August 2013): 16.

95. “Article V,” Treaty of Mutual Cooperation and Security between Japan and the United States of America, January 19, 1960. <http://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html>.

96. U.S. Senate Foreign Relations Committee, *Hearing on Maritime Territorial Disputes and Sovereignty Issues in Asia*, testimony of Kurt Campbell, 112th Cong., 2nd sess., September 20, 2012.

97. U.S. Senate Foreign Relations Committee, *Hearing on Maritime Territorial Disputes and Sovereignty Issues in Asia*, testimony of Kurt Campbell, 112th Cong., 2nd sess., September 20, 2012.

98. Bonnie Glaser, “Armed Clash in the South China Sea: Contingency Planning Memorandum No. 14,” (New York, NY: Council on Foreign Relations, April 2012). <http://www.cfr.org/world/armed-clash-south-china-sea/p27883>; U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of David Lampton, February 7, 2013.

99. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Wallace Gregson, February 7, 2013.

100. U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of David Lampton, February 7, 2013; U.S.-China Economic and Security Review Commission, *Hearing on China's New Leadership and Implications for the United States*, written testimony of Michael Auslin, February 7, 2013.

101. Jonathan Greenert, “Sea Change: The Navy Pivots to Asia,” *Foreign Policy*, November 14, 2012. http://www.foreignpolicy.com/articles/2012/11/14/sea_change; U.S. Senate Foreign Relations Committee, *Hearing on Maritime Territorial Disputes and Sovereignty Issues in Asia*, testimony of Kurt Campbell, 112th Cong., 2nd sess., September 20, 2012.

102. Kenneth Lieberthal and Wang Jisi, *Addressing U.S.-China Distrust* (Washington, DC: The Brookings Institution, April 2012). http://www.brookings.edu/~media/research/files/papers/2012/3/30%20us%20china%20lieberthal/0330_china_lieberthal.pdf.

103. For more information on these regimes, see Kimberly Hsu and Craig Murray, *China's Expanding Operations in Foreign Exclusive Economic Zones* (Washington, DC: U.S.-China Economic and Security Review Commission, June 2013). <http://www.uscc.gov/Research/china%E2%80%99s-expanding-military-operations-foreign-exclusive-economic-zones>.

RECOMMENDATIONS

China's Cyber Activities

The Commission recommends:

- Congress adopt legislation clarifying the actions companies are permitted to take regarding tracking intellectual property stolen through cyber intrusions.
- Congress amend the Economic Espionage Act (18 U.S.C. § 1831–1839) to permit a private right of action when trade secrets are stolen.
- Congress support the Administration's efforts to achieve a high standard of protection of intellectual property rights in the Trans-Pacific Partnership and the Transatlantic Trade and Investment Partnership.
- Congress encourage the Administration to partner with other countries to establish an international list of individuals, groups, and organizations engaged in commercial cyber espionage. The Administration and partner governments should develop a process for the list's validation, adjudication, and shared access.
- Congress urge the Administration to continue to enhance its sharing of information about cyber threats with the private sector, particularly small- and medium-sized companies.
- Congress direct the Administration to prepare an inventory of existing federal use of cloud computing platforms and services and determine where the data storage and computing services are geographically located. Such inventory should be prepared annually and reported to the appropriate committees of jurisdiction.
- Congress urge the Administration to expedite progress in its implementation of Section 806 of the National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383), which was intended to enhance the Department of Defense's ability to address supply chain risks.

China's Maritime Disputes

The Commission recommends:

- Congress fund the U.S. Navy's shipbuilding and operational efforts to increase its presence in the Asia Pacific to at least 60 ships and rebalance homeports to 60 percent in the region by 2020 so that the United States will have the capacity to maintain readiness and presence in the Western Pacific, offset China's

growing military capabilities, and surge naval assets in the event of a contingency.

- Congress fund Departments of Defense and State efforts to improve the air and maritime capabilities of U.S. partners and allies in Asia, particularly with regard to intelligence, surveillance, and reconnaissance, to improve maritime domain awareness in the East and South China Seas.
- Congress urge the Department of Defense to continue to develop the U.S.-China maritime security relationship in order to strengthen strategic trust. The relationship should be within the bounds of the National Defense Authorization Act for Fiscal Year 2000 (Public Law 106–65) and based on the principles of reciprocity and transparency.
- Congress fund U.S. Coast Guard engagement efforts with coast guard and maritime law enforcement agencies in the Western Pacific to increase understanding among civilian maritime bodies in the Asia Pacific.