

CHAPTER 2

CHINA'S ACTIVITIES DIRECTLY AFFECTING U.S. SECURITY INTERESTS

SECTION 1: MILITARY AND SECURITY YEAR IN REVIEW

Introduction

This section provides an overview of the most relevant Chinese military and security developments since the Commission's *2010 Annual Report to Congress*. It is divided into three subsections: military developments, China's recent foreign policy activities, and updates on China's cyber activities. This year's military developments section describes progress in China's military modernization efforts, official statements from Beijing concerning its security interests, recent People's Liberation Army (PLA) activities, and the U.S.-China military-to-military relationship. China's foreign policy subsection focuses on China's assertive behavior in the South China Sea over the past year. The final subsection describes China's recent cyber activities, both at home and abroad.

Military Developments in 2011

Over the past year, several notable developments involving China's military have occurred. China's military modernization continued to progress, as evidenced by a series of firsts: China conducted test flights of its first stealth fighter, conducted a sea trial of its first aircraft carrier, and may have deployed the world's first ballistic missile capable of hitting moving ships at sea. China also conducted a major noncombatant evacuation of its citizens from Libya, the first involving the PLA. The past year also saw the resumption of military-to-military engagement between the United States and China, with three consecutive meetings between senior U.S. and Chinese military officials. The following subsection describes these events.

Military Modernization

J-20 stealth fighter

In January 2011, China conducted the inaugural test flight of its next-generation fighter aircraft, the J-20. Although the flight attracted considerable attention in and outside of China, few details emerged about the fighter. Developed at the Chengdu Aircraft Design Institute, the plane appears to have a sufficient combat radius

to operate beyond China's borders and will likely have midair refueling capabilities.* The fighter's other features, such as the speed and altitude at which it can travel, and its thrust capabilities and maneuverability, could not be determined by foreign observers of the test. Each of these capabilities depends on the J-20's engine, a component that the manufacturer may not yet have finally selected.¹ As described in the Commission's 2010 Report, turbofan engine development remains a persistent weakness in China's aviation industry,² which raises questions about the J-20's performance potential if it relies on domestic technology. The use of a Russian engine is one possibility to overcome any problems with an indigenous Chinese engine.† The U.S. Department of Defense (DoD) does not anticipate the J-20 to be operational prior to 2018.³

The J-20's design has led to considerable speculation about its stealth capability, or ability to evade radar detection. This capability consists primarily of the plane's configuration and design, as well as the materials and coatings it incorporates.‡ Aspects of the J-20's design, such as the forewings ("canards"), engine cover ("cowling"), jet and pelvic fin, and engine nozzles raise questions about whether it would successfully evade advanced radars.⁴ In addition to design, the use of certain materials and coatings absorb radar signals, which can increase stealth. Pictures and video of the J-20 do not provide enough information to determine whether China's defense industries have mastered this aspect of advanced aircraft design. However, in late January 2011, Croatia's former military chief of staff stated that China had possibly received the stealth technology for the J-20 from parts of a U.S. F-117 stealth bomber shot down over Serbia in 1999.§

U.S. Corporate Participation in China's Aviation Programs in 2011

Several western aviation firms established or deepened ties to Chinese state-owned aviation firms in 2011. For example, General Electric (GE) Aviation and the state-owned Aviation Industry Corporation of China announced in January a joint venture

* "Combat radius" refers to the distance a plane can travel to a mission area, execute a mission, and have adequate fuel to return to its base. Combat radius estimates for the J-20 range from 1,000 to 1,500 nautical miles. Carlo Kopp, "An Initial Assessment of China's J-20 Stealth Fighter," *China Brief* 11:8 (May 6, 2011): 9. http://www.jamestown.org/uploads/media/cb_11_8_04.pdf.

† Two J-20 demonstrators may exist: one with a Chinese WS-10A engine and one with a Russian-made AL-F1FN engine. Notably, China has been unable to place the WS-10 series engine into serial production even several years after its development plans had been completed. As recently as last year, China requested advanced 117S engines from Russia. Tai Ming Cheung, "What the J-20 Says About China's Defense Sector," *Wall Street Journal*, January 13, 2011. http://blogs.wsj.com/chinarealtime/2011/01/13/what-the-j-20-says-about-chinas-defense-sector/?mod=rss_WSJBlog&mod=chinablog.

‡ This discussion includes passive design features but not active measures, such as electronic warfare, that might be used to evade radar detection.

§ China's state-run newspaper, *Global Times*, referred to this claim as a "smear." BBC, "China stealth fighter 'copied parts from downed US jet,'" January 24, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-12266973>; BBC, "China newspaper rejects J-20 stealth jet claim," January 25, 2011. <http://www.bbc.co.uk/news/world-asia-pacific-12274807>. China also reportedly gained access to U.S. stealth materials from Pakistan following the downing of a U.S. stealth helicopter used for the raid on Osama Bin Laden's compound in May 2011, although the event took place after the J-20's maiden voyage. Reuters, "Pakistan let China see crashed U.S. 'stealth' copter," August 14, 2011. <http://www.reuters.com/article/2011/08/14/us-pakistan-china-usa-idUSTRE77D2BT20110814>.

U.S. Corporate Participation in China's Aviation Programs in 2011—Continued

for integrated avionics, which, according to a GE press release, will transfer ownership of GE's existing civilian avionics operations to the joint venture and be "the single route-to-market for integrated avionics systems for both GE and AVIC [Aviation Industry Corporation of China]." The press release further describes the deal, stating that "the new AVIC [Aviation Industry Corporation of China] and GE joint venture company will develop and market integrated, open architecture avionics systems to the global commercial aerospace industry for new aircraft platforms. This system will be the central information system and backbone of the airplane's networks and electronics and will host the airplane's avionics, maintenance, and utility functions."⁵ Notably, GE characterized the joint venture's work in China as research and development "to come up with breakthrough technologies and create 'new IP [intellectual property] and new technology'." In describing the Aviation Industry Corporation of China, the press release also noted that "[t]he company has also developed strong capabilities to supply avionics products to various models of aircrafts, both for military and civil use."⁶ Of import, because GE is also providing the engines for the C919, through a joint venture with the French firm Snecma (Safran Group),⁷ improving the C919's avionics will make it more marketable, which will in turn allow GE to sell more engines. It is worth noting that as a Commission-sponsored report details, both engine development and avionics are areas where China's aviation industry continues to have problems and currently must rely on foreign imports.⁸

Boeing also undertook several new projects with the Aviation Industry Corporation of China in 2011. In June, the firms announced the creation of a new Manufacturing Innovation Center in Xi'an, which would, among other things, "support AVIC's [Aviation Industry Corporation of China] goals of improving its manufacturing and technological capabilities and the competitiveness of its affiliated factories to achieve global Tier-1 supplier status."⁹ In addition, Boeing announced in April that it planned to double the capacity of a joint venture with the Aviation Industry Corporation of China, called Boeing Tianjin, which produces composites.¹⁰ One of the joint venture's customers is the Xi'an Aviation Industry Corporation,¹¹ which manufactures components for civil aircraft and produces military aircraft, such as the JH-7A fighter bomber and the H-6 bomber, for the PLA.¹²

Aircraft carrier program

In July 2011, China officially revealed its long-suspected aircraft carrier program when it publicly announced that it was developing an aircraft carrier.¹³ A month later, China conducted a sea trial of its first aircraft carrier off the port of Dalian.¹⁴ Not an indigenously developed vessel, China's aircraft carrier is a renovated Soviet *Kuznetsov*-class carrier (the *Varyag*) purchased from Ukraine in 1998. At the time of its purchase, a Hong Kong company, with al-

leged ties to the Chinese government and the PLA, purchased the carrier without engines, rudders, or weapons, ostensibly for use as a floating casino off the island of Macau.¹⁵ After several years of setbacks, in 2002 the *Varyag* finally arrived at the Chinese port of Dalian, its current homeport.*¹⁶ Although it is unclear when the PLA officially gained control over the vessel, China has been working since 2004 to make the carrier operational. After the sea trial, the *Varyag* returned to Dalian for further work.¹⁷ According to unnamed PLA sources, the carrier will not be launched officially until October 2012.¹⁸ Unconfirmed rumors also posit that China is constructing one or more indigenous carriers for a future aircraft carrier fleet.¹⁹ China is also developing the aircraft to be deployed along with the aircraft carriers. In April 2011, Internet photos revealed a test version of a carrier-based fighter, the J-15.²⁰ According to analysts, this aircraft appears to be a modified version of China's J-11B fighter, which in itself is an unlicensed adaptation of Russia's SU-27 Flanker. The J-15 is not expected to be deployed before 2016.²¹ The PLA Navy is also developing the means to train future pilots in the dangerous task of taking off from and landing on an aircraft carrier. In June 2011, China's Guizhou Aviation Industry conducted the test flight of an advanced trainer aircraft, the JT-9 (also referred to as the JL-9H).²² China has also constructed at least two land-based pilot training centers to teach PLA Navy pilots how to land on an aircraft carrier. Both centers have ski-jump platforms that mimic the shape of the *Varyag's* deck.[†]²³

The People's Republic of China's (PRC) official position about the use of its aircraft carrier is that it will be used for "scientific research, experiment and training."²⁴ This corresponds with the U.S. Department of Defense's view, which maintains that China's first aircraft carrier "will likely serve initially as a training and evaluation platform and eventually offer a limited operational capability."²⁵ However, a Chinese Ministry of Defense spokesman noted in July 2011 that a carrier could be used for offensive or defensive purposes as well as for disaster relief and that China was pursuing its carrier program "in order to increase its ability to protect national security and world peace."²⁶ Another article in China's official press says that aircraft carriers are vital to China given China's "vast territorial waters" and the current inability of the PLA Navy to safeguard this region. The article also points out China's need to safeguard its global interests and protect the sea lanes upon which China's continued economic development rests.²⁷

China's aircraft carrier development program currently poses little direct threat to the United States and is likely more of a concern to regional maritime states. In testimony to the U.S. Senate, Robert F. Willard, commander of the U.S. Pacific Forces, stated

* Because the *Varyag* lacked engines and rudders, Turkish authorities were reluctant to allow it to be towed through the Bosphorus Strait, for fear of damaging the narrower portions of the strait. Ian Story and You Ji, "China's Aircraft Carrier Ambitions: Seeking Truth from Rumors," *Naval War College Review* LVII: 1 (Winter 2004): 83.

† Given the small flight deck of carriers compared to land-based runways, aircraft rely upon two means for successfully lifting off from an aircraft carrier. Conventional aircraft carriers, such as U.S. carriers, have a catapult system that assists the aircraft in reaching the requisite speed prior to take-off. Another method is to install a slight ramp on the end of the deck, referred to as a "ski-jump," that propels the aircraft up and out as it exits the ship's deck. China's *Varyag* aircraft carrier has a ski-jump type deck. Michael Wines, "Chinese State Media, in a Show of Openness, Print Jet Photos," *New York Times*, April 25, 2011. <http://www.nytimes.com/2011/04/26/world/asia/26fighter.html>.

that he was not concerned about the military impact of the carrier. However, Admiral Willard did note that it could have an impact on perceptions of China in the region.²⁸ When the *Varyag* is deployed, it will make China one of only ten countries that operate aircraft carriers, none of which are countries with which China has maritime disputes.* Possession of an aircraft carrier would allow China to project force throughout the region, especially into the far reaches of the South China Sea, something it currently cannot fully do. Possibly in an attempt to temper regional fears of China's aircraft program, China's state-run news outlet Xinhua wrote, "[t]here should be no excessive worries or paranoid feelings on China's pursuit of an aircraft carrier, as it will not pose a threat to other countries, and other countries should accept and be used to the reality that we are developing the carrier."²⁹

Given the complexity of conducting carrier operations, it is expected to be several years before China's aircraft carrier will be fully operational.³⁰ According to Michael McDevitt, a retired rear admiral in the U.S. Navy, the PLA Navy will face a number of challenges in the coming years integrating carrier and air wing operations.³¹ Additionally, as defense analysts Nan Li and Christopher Weuve noted, "An aircraft carrier is not a solo-deploying ship. To be survivable in an intense combat environment, it needs escorts to protect it."³² China has taken steps to develop such support systems, but their capabilities are uneven. For example, according to the same analysis, "While China has acquired new surface combatants with sophisticated antisurface and antiair capabilities, it continues to lag behind in the area of ASW [anti-submarine warfare]," which could seriously challenge carrier operations in certain scenarios.³³

The DF-21D antiship ballistic missile

Over the past year, several developments concerning China's antiship ballistic missile, the DF-21D, have occurred. In December 2010, Admiral Willard described in the following exchange with a reporter how the DF-21D was possibly operational:

Reporter: Let me go into China's anti-access/area denial (A2/AD) capabilities. What is the current status of China's anti-ship ballistic missile development, and how close is it to actual operational deployment?

Admiral Willard: The anti-ship ballistic missile system in China has undergone extensive testing. An analogy using a Western term would be 'initial operational capability,' whereby it has—I think China would perceive that it has—an operational capability now, but they continue to develop it. It will continue to undergo testing, I would imagine, for several more years.

Reporter: China has achieved IOC [initial operational capability]?

*The other nine countries currently possessing aircraft carriers are Brazil, France, India, Italy, Russia, Spain, Thailand, the United Kingdom, and the United States. China currently has maritime disputes in the East China Sea with Japan, and in the South China Sea with Brunei, the Philippines, Malaysia, Taiwan, and Vietnam.

*Admiral Willard: You would have to ask China that, but as we see the development of the system, their acknowledging the system in open press reporting and the continued testing of the system, I would gauge it as about the equivalent of a U.S. system that has achieved IOC [initial operational capability].*³⁴

In July 2011, Chinese sources officially confirmed the development of the DF-21D for the first time. In an article in China's state-controlled *China Daily* newspaper, PLA Major General Chen Bingde, chief of the General Staff, acknowledged that the PLA is developing the DF-21D. However, Major General Chen dismissed the notion that the missile is currently operational, stating that the DF-21D "is still undergoing experimental testing" and that "it is a high-tech weapon and we face many difficulties in getting funding, advanced technologies and high-quality personnel, which are all underlying reasons why it is hard to develop this." The *China Daily* article further noted that the DF-21D is "a ballistic missile with a maximum range of 2,700 kilometers (km) and the ability to strike moving targets—including aircraft carriers—at sea."³⁵ Of import, the stated range of this missile is significantly greater than the DOD's estimate of "exceeding 1,500 km."³⁶ It is unclear what accounts for this discrepancy, although in response to a Commission question, the DoD attributed the differences in stated ranges to possible erroneous reporting by the Chinese press and remained "confident" about the department's original assessment.³⁷ (For more on the DF-21D and how it could play an integral part in China's efforts to deny U.S. military forces the ability to operate freely in the western Pacific, see chap. 2, sec. 2, of this Report.)

Official Statements

2011 defense budget

In March 2011, China officially released its defense budget for the year. According to Chinese sources, China's defense budget for 2011 is \$91.5 billion, a 12.7 percent increase over 2010.³⁸ This represents the 20th increase in as many years. According to the DoD, between 2000 and 2010 "China's officially disclosed military budget grew at an average of 12.1 percent in inflation-adjusted terms," a percentage value that the DoD also notes tracks closely with the growth in China's gross domestic product for the same period.³⁹ However, western analysts readily discount Chinese figures for its defense budget as inaccurate. Because these statistics do not take into account all defense expenditures, the likely figure is much higher.⁴⁰ In testimony to the Commission, Mark Stokes, a former lieutenant colonel in the U.S. Air Force and current executive director of the Project 2049 Institute, stated, "While the PLA deserves credit for greater transparency, key areas of defense expenditure, such as research and development, remain opaque."⁴¹ China's official defense budget also does not include foreign procurement.⁴² Abraham Denmark, then fellow at the Center for New American Security, testified to the Commission that "given China's practice of significantly under-reporting defense expenditures, it is safe to estimate China's actual annual spending on its military power to be well over \$150 billion."⁴³ In its 2011 report to Con-

gress, the DoD noted that China's 2010 defense budget was likely about twice what Beijing reported, at over \$160 billion.⁴⁴

China's 2011 defense white paper

On March 31, 2011, China released its seventh biannual defense white paper, *China's National Defense in 2010*, an authoritative statement of Beijing's views of China's security environment. This report posits a relatively optimistic picture, noting that "China is still in the period of important strategic opportunities for its development, and the overall security environment for it remains favorable." However, the paper lists several areas that Beijing views as a potential threat to China's stability and security: Taiwan, independence movements in China's Tibet and Xinjiang provinces, China's disputed maritime claims, nontraditional security concerns,* and growing opposition to China stemming from China's rise. Of import, the white paper singles out the United States (the only nation mentioned by name) in the section on "threats and challenges" because of U.S. arms sales to Taiwan.⁴⁵

As an important piece of China's strategic messaging, the primary audience for China's defense white papers is foreign actors.⁴⁶ This iteration in particular appears to be an attempt to allay fears of China's growing military capabilities in the region.⁴⁷ According to the Congressional Research Service, "The overall purpose of the defense white paper seems to be to counter what Beijing calls the 'China Threat Theory' and to affirm that the PRC remains a peaceful power pursuing 'Peaceful Development' with a military that is 'defensive in nature.'" ⁴⁸ CNA China Studies Center, a Washington, DC-based, research institute, described how:

*The main message of the 2010 edition for external audiences is one of reassurance. The message being conveyed . . . is that Beijing has not changed its defensive military posture despite its growing military capabilities and its various extraterritorial military deployments. . . . These messages of assurance come on the heels of a period of about two years during which Chinese foreign policy and security policy initiatives were described by foreign observers as 'assertive' or uncharacteristically muscular. Consequently, one likely objective of this paper is to calm the waters, especially in the Asia-Pacific region.*⁴⁹

Despite the stated goal of providing more transparency on China's military modernization efforts and intentions, the defense white paper falls short.⁵⁰ Phillip C. Saunders, director of studies at the Center for Strategic Research at the U.S. National Defense University, asserted that the 2010 white paper is less transparent than previous iterations.⁵¹ The report provides few new details, leaving many critical questions unanswered.⁵² For example, Shirley A. Kan, an Asian Defense Security analyst at the Congressional Research Service, noted that China's 2010 defense white paper provided:

*The defense white paper lists the following nontraditional security concerns: terrorism, energy resources, financial problems, information security, and natural disasters. Information Office of the State Council, *China's National Defense in 2010* (Beijing, China: March 2011).

*no details on satellites, anti-satellite (ASAT) weapons, space program, aircraft carriers, ships, strategic and other submarines, fighters including the J-20 fighter that was flight tested during Defense Secretary Robert Gates' visit in January 2011, aerial refueling for operations far from China, new nuclear-armed intercontinental ballistic missiles, anti-ship ballistic missiles, land attack cruise missiles, or short-range ballistic missiles threatening Taiwan.*⁵³

Military Operations

Antipiracy operations off the Horn of Africa

In July 2011, the PLA Navy dispatched its ninth task force to conduct escort missions through the pirate-infested waters of the Gulf of Aden.⁵⁴ As the Commission noted in its 2009 report, since January 2009, the PLA Navy has assisted United Nations (UN) antipiracy operations around the Horn of Africa.⁵⁵ The PLA Navy's current task force consists of a destroyer, a frigate, a replenishment ship, and a small contingent of marines. According to Chinese statistics, to date the task forces have escorted approximately 4,000 Chinese and foreign-flagged cargo vessels in the region.⁵⁶ Since early 2010, the task forces have conducted regular monthly port calls for replenishment and overhaul, stopping mainly at three locations: Port of Salalah (Oman), Port of Djibouti (Djibouti), and Port of Aden (Yemen). PLA Navy ships from the task forces have also conducted at least 19 friendly port calls during their deployment in support of the China's military diplomacy efforts. During five of these port visits, the PLA Navy conducted joint maritime drills with the host nation's naval forces.*⁵⁷

The PLA Navy, similar to vessels from Russia, India, and Japan, primarily conducts antipiracy escort missions of civilian cargo vessels and does not participate in regional counterpiracy operations.† However, the PLA Navy does coordinate its antipiracy activities with the main counterpiracy task force, Combined Task Force 151, through a separate, monthly gathering called Shared Awareness and Deconfliction. China has even expressed an interest in assuming the chairmanship of this latter institution.⁵⁸ During a May 2011 visit to the United States, Major General Chen opened the door for the possible participation of Chinese forces in counterpiracy operations, stating that “for counterpiracy campaigns to be effective, we should probably move beyond the ocean and crash their bases on the land.”⁵⁹

Evacuation of Chinese civilians from Libya, February–March 2011

During the fighting between pro-Qaddafi and anti-Qaddafi forces in Libya in February and March 2011, the Chinese government conducted what it considers to be its “largest and the most complicated overseas evacuation ever” and the first involving the

* The maritime drills were conducted with the navies of Italy, Pakistan (twice), Singapore, and Tanzania. Open Source Center, “OSC Interactive Map: Chinese PLA Navy Escort Mission Port Calls,” *OSC Summary* (May 2, 2011). OSC ID: FEA20110503017394. <http://www.opensource.gov>.

† Counterpiracy operations are operations that seek actively to suppress piracy, as opposed to antipiracy operations, which are operations to prevent and deter piracy.

PLA.⁶⁰ Prior to the conflict, China had approximately 36,000 citizens working in Libya for 75 Chinese companies. As the fighting intensified, China's citizens and company facilities increasingly came under attack.⁶¹ In an effort to ensure their safety, the Chinese government organized a complex evacuation operation that, according to the Chinese Ministry of Foreign Affairs, involved "91 domestic chartered flights, 12 flights by military airplanes, five cargo ferries, one escort ship, as well as 35 rented foreign chartered flights, 11 voyages by foreign passenger liners and some 100 bus runs." After eight days, "all Chinese in Libya who desired to go back and whose whereabouts were known by the foreign ministry—35,860 in number, had been evacuated."⁶²

This was the first noncombatant evacuation operation from an active combat zone in which the PLA participated. On February 24, the PLA Navy dispatched the guided missile frigate *Xuzhou*, then participating in antipiracy operations off the Horn of Africa, to assist in the evacuation efforts. Arriving in the Mediterranean, the frigate began escorting chartered civilian ships evacuating Chinese citizens to Greece.⁶³ In another first, the PLA Air Force also dispatched four IL-76 transport aircraft to assist in the evacuation process. These aircraft, dispatched from China's westernmost province, Xinjiang, on February 28, began evacuating people to Khartoum, Sudan, the next day. According to Chinese reports, the aircraft flew over Pakistan, Oman, Saudi Arabia, and Sudan before landing in Sabha, Libya. During the flight to Libya, the aircraft refueled twice, in Karachi, Pakistan, and Khartoum, Sudan.⁶⁴

U.S.-China Military-to-Military Relations

Secretary of Defense Robert F. Gates' visit to China

On January 9–12, 2011, then U.S. Secretary of Defense Robert F. Gates visited China, marking the resumption of U.S.-China military-to-military relations that China cut off following the Obama Administration's January 2010 notification to Congress about potential U.S. arms sales to Taiwan. During his visit, Secretary Gates met with Chinese Minister of Defense General Liang Guanglie and General Secretary of the Chinese Communist Party (CCP) and President Hu Jintao and visited the headquarters of the Second Artillery (the PLA's strategic rocket forces). Over the course of the trip, the leaders discussed tensions on the Korean Peninsula, nuclear strategy, and the possible development of joint military exercises in maritime search and rescue, humanitarian assistance, disaster relief, counterpiracy, and counterterrorism, among other things.⁶⁵

The stated goal of Secretary Gates' trip was to initiate a regular, bilateral defense dialogue over contentious issues like nuclear policy, missile defense, cybersecurity, and space security in order to avoid future miscommunication and miscalculation.⁶⁶ Observers perceived that this goal was only partially achieved, as General Liang declined to put forth a timetable for such talks, only agreeing that defense exchanges between the two countries would occur in the first half of 2011 and that the PLA was "studying" the proposal for a regular dialogue.⁶⁷ After the trip, Secretary Gates stated that he was satisfied with the overall visit, saying that "this is

not an area where you will see dramatic breakthroughs and new headlines, but rather evolutionary growth.”⁶⁸

The unexpected highlight of the trip was the test flight of China’s new J–20 stealth fighter aircraft, which took place hours before Secretary Gates’ meeting with President Hu. When Secretary Gates inquired about the test flight, President Hu claimed to be unaware that it had occurred.⁶⁹ A Chinese defense ministry deputy director stated that the test was part of a “normal working schedule” and that it was not related to Secretary Gates’ visit.⁷⁰ According to the Commission testimonies of Andrew Scobell, senior political scientist at the RAND Corporation, and Mr. Denmark, it is inconclusive whether or not the test was planned to occur because of the visit.⁷¹ The “surprise” test flight raised concerns that the PLA might be acting independently of China’s civilian leaders. In a speech in Tokyo following his trip to China, Secretary Gates noted that “[o]ver the last several years we have seen some signs of ... a disconnect between the military and the civilian leadership [in China].” He added that he was confident that President Hu and the CCP remained fully in control of the military.⁷² Dr. Scobell, however, opined that “[f]undamentally, the J–20 episode underscores the fact that civilian control of the military is underinstitutionalized in 21st Century China.”⁷³

PLA Chief of Staff Chen Bingde’s visit to the United States

China’s pledge to enhance military-to-military exchanges in 2011 was upheld in May when the PLA Chief of General Staff, Major General Chen Bingde, visited the United States. During his trip, Major General Chen toured four military bases;* delivered a speech at the U.S. National Defense University; and held talks with Secretary Gates, Secretary of State Hillary Rodham Clinton, and Admiral Mike Mullen, then chairman of the Joint Chiefs of Staff. He and his delegation also attended a goodwill concert featuring performances of the official bands of the U.S. Army and the PLA.⁷⁴

A joint statement presented by Admiral Mullen and Major General Chen outlined six bilateral agreements reached from the visit: (1) a consensus that the two sides would work together within the framework agreed by President Hu and President Barack Obama; (2) the establishment of a direct telephone line between the Chinese Ministry of Defense and the U.S. Department of Defense; (3) plans to conduct joint naval exercises in the Gulf of Aden as part of the international antipiracy effort; (4) plans to conduct a humanitarian disaster rescue and relief joint training exercise in 2012; (5) an agreement to exchange medical information and conduct joint medical rescue training exercises; and (6) an invitation from China for the U.S. Army Band and shooting team to visit China.⁷⁵

Although the two sides were able to reach several points of consensus, a number of differences were highlighted. During a press conference, General Chen commented on China’s opposition to sev-

*General Chen toured Naval Station Norfolk, Virginia; Fort Stewart, Georgia; Nellis Air Force Base, Nevada; and the National Training Center at Fort Irwin, California. Agence France-Presse, “U.S. Rolls Out Red Carpet for China Military Chief,” May 14, 2011. <http://www.defensenews.com/story.php?i=6502345>.

eral U.S. military policies, including arms sales to Taiwan, reconnaissance activities along Chinese coasts by U.S. military aircraft and vessels, and restrictions on U.S. exports of high technologies to China.⁷⁶ Of note, some U.S. observers, including Members of Congress, were critical of Major General Chen's visit to U.S. military bases, saying those visits might violate the *2000 National Defense Authorization Act*, which bans Chinese military visitors to the United States from "inappropriate exposure" to information that could be used to enhance the PLA's capacity to conduct combat operations.⁷⁷

Admiral Mullen's visit to China

Admiral Mullen reciprocated Major General Chen's visit in July 2011. Admiral Mullen and his 39-person delegation visited Beijing as well as Shandong and Zhejiang provinces, where they met with a number of high-level government and military officials, including Vice President (and likely future President and Party Secretary) Xi Jinping. On the trip, Admiral Mullen visited units in the army, navy, air force, and the Second Artillery (strategic rocket forces) and was introduced to several pieces of Chinese military technology, including the Su-27, one of China's most advanced operational fighter jets, and a Type-39A *Yuan*-class diesel-electric submarine.⁷⁸ At a joint press conference, Admiral Mullen and Major General Chen announced plans to hold antipiracy maneuvers in the Gulf of Aden by year's end, to hold talks on operational safety in Hawaii and China, and to plan joint humanitarian relief exercises in 2012.⁷⁹

Some divisive issues punctuated the visit. During a press conference, General Chen three times criticized recent joint naval exercises between the United States, Australia, and Japan in the South China Sea. He also raised complaints over controversial non-military issues such as the attitudes of some American politicians toward China and a U.S. visit by the Dalai Lama.⁸⁰ Admiral Mullen expressed concern over North Korea's recent provocative comments and actions and encouraged Beijing to use its strong ties with Pyongyang to ensure stability on the Korean Peninsula.⁸¹

Implications for the United States

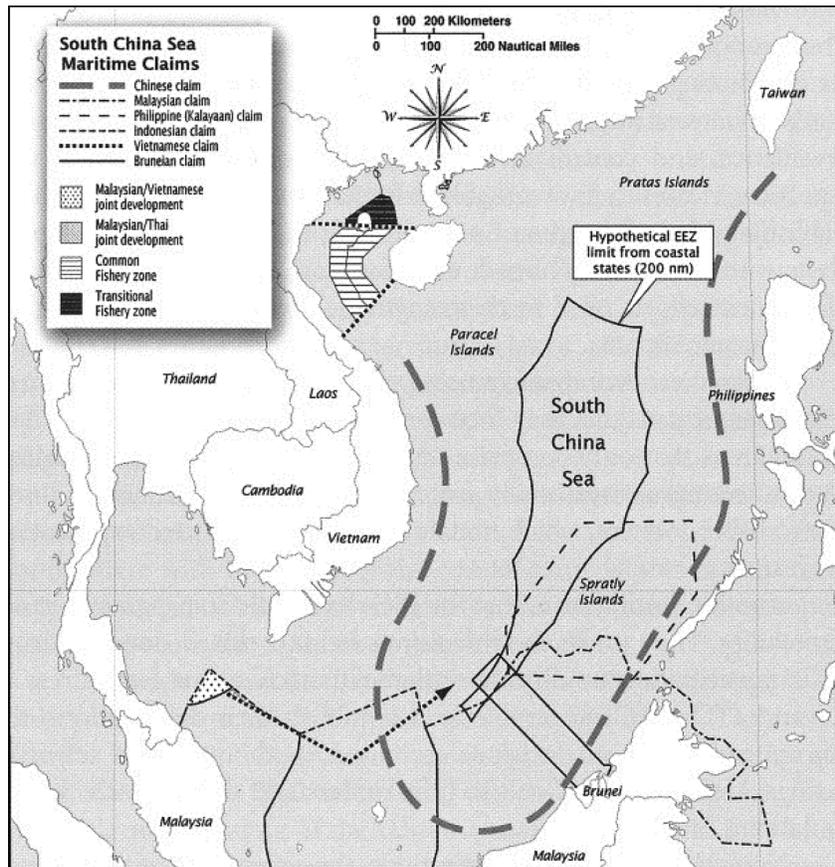
As demonstrated above, China has progressed substantially over the past year in its military modernization efforts. These developments show that China is attempting to increase its ability to project power in the region. Developments in China's stealth fighter, aircraft carrier and carrier aircraft, and antiship ballistic missile programs, when completed, will provide the PLA with an increased capacity to exert control over the western Pacific and threaten regional states and U.S. forces operating within the region in the event of a conflict. These developments also embolden China and the PLA in its interactions with other nations, as evidenced during recent U.S.-China military-to-military dialogues.

Recent Chinese Assertiveness in the South China Sea

Tension between China and other claimants in the South China Sea territorial disputes [see figure 1, below] has waxed and waned in recent years, with periods of confrontation and intimidation followed by attempts at reconciliation and confidence building.* China displayed increasing territorial aggression in the spring and summer months of 2011. In June, Ian Storey, fellow at the Institute for Southeast Asian Studies in Singapore, noted that tensions in the disputed seas were at their highest levels since the end of the Cold War.⁸² Notwithstanding China's intermittent displays of cooperation, China's expanding military, commercial, and rhetorical assertiveness in the South China Sea indicates that China is unlikely to concede any of its sovereignty claims in the area.⁸³ Expert witnesses testified to the Commission that China's patterns of assertiveness in the South China Sea call into question its "peaceful rise" as well as its long-term views toward its regional neighbors and the United States.⁸⁴

* Brunei, China, Malaysia, the Philippines, Taiwan, and Vietnam are claimants in maritime disputes in the South China Sea. For information on developments in the South China Sea in 2009 and 2010, see U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), pp. 132–137.

Figure 1: Territorial Disputes in the South China Sea



Source: James Clad, Sean M. McDonald, and Bruce Vaughn, eds., *The Borderlands of South-east Asia* (Washington, DC: National Defense University, 2011), p. 121. Note: Indonesia does not consider itself a claimant to any dispute in the South China Sea, even though its territorial claims in the region overlap with China's. Permanent Mission of the Republic of Indonesia to the United Nations, Circular Note No. 480/POL-703/VII/10, July 8, 2010. http://www.un.org/Depts/los/cles_new/submissions_files/mysvnm33_09/idn_2010re_mys_vnm_e.pdf.

The following are examples of China's assertiveness in the South China Sea in the past year:

Obstruction of resource exploration activities—Chinese vessels obstructed resource exploration activities in the claimed territories of other countries at least three times in the first half of 2011. Each of these instances may constitute a violation of the United Nations Convention on the Law of the Sea, which allows any country sovereign rights to conduct economic or resource management activities in an exclusive economic zone (EEZ) up to 200 nautical miles from its shores and to which China is a signatory.[†] In March 2011,

[†] An exclusive economic zone is the maritime territory of a coastal state out to 200 nautical miles, where the coastal state enjoys "sovereign rights for the purpose of exploring and exploit-

Continued

two Chinese patrol boats aggressively approached and chased away a seismic survey vessel conducting an assessment of a gas field in the Philippines' EEZ near the disputed Spratly Islands. The vessel, chartered by the British energy consortium Forum Energy, was conducting work on behalf of the Philippine government.⁸⁵ The incident prompted harsh responses from the Philippines in the following months. Philippine President Benigno Aquino III announced plans to take the dispute over the Spratly Islands to the United Nations International Tribunal on the Law of the Sea.⁸⁶ He also vowed to bolster the Philippines' military power in order to protect its economic interests in the face of growing Chinese assertiveness. In June, the Philippines announced a \$252 million upgrade for its navy and deployed its largest warship to patrol the South China Sea.⁸⁷ In September, the Philippines allocated an additional \$118 million for the purchase of a navy patrol vessel, six helicopters, and other hardware to secure the perimeter of the country's largest gas extraction project, which is located 50 miles from a Philippine island near waters claimed by China.⁸⁸ President Aquino also called on the United States, a treaty partner, to help the Philippines stand up to the Chinese.⁸⁹

Vietnamese officials reported that Chinese boats harassed Vietnamese oil and gas surveying ships operating in the South China Sea on two separate occasions in 2011. In the first incident, which occurred in late May, state oil company PetroVietnam alleged that while it was conducting seismic operations, Chinese airplanes harassed the company's ships, and three Chinese marine surveillance vessels subsequently cut the company's survey cables.⁹⁰ The second incident occurred in June and involved a Chinese patrol boat cutting the cable of a Vietnamese oil-drilling research vessel.⁹¹ Both incidents occurred in Vietnam's EEZ, less than 200 nautical miles from the Vietnamese coast, and the second of the incidents occurred more than 600 nautical miles from China's island province of Hainan.⁹² In previous years, Chinese patrol boats typically only harassed fishermen, not oil and gas vessels.⁹³

Deep sea oil rig stationed in the South China Sea—China has built an advanced, deep-water oil rig that it plans to use in the South China Sea. Launched in the summer of 2011, the \$1 billion oil rig, owned by the Chinese state-owned oil company China National Offshore Oil Corporation, is China's first deep-water drilling rig and allows China to drill in deeper waters than ever before.⁹⁴ The exact location of the rig was unclear at the time of the publication of this Report. The Philippines has expressed concern and has asked China's embassy to clarify the exact location of the planned rig.⁹⁵

Harassment of Vietnamese and Philippine fishermen—Vietnamese and Philippine fishermen reported an uptick in harassment by Chinese maritime patrol boats in early 2011, including the threatening of fishermen and the seizure and confiscation of fish

ing, conserving and managing the natural resources, whether living or non-living, of the waters superjacent to the sea-bed and of the sea-bed and its subsoil, and with regard to other activities for the economic exploitation and exploration of the zone, such as the production of energy from the water, currents and winds." United Nations, "Exclusive Economic Zones," *United Nations Convention on the Law of the Sea* (New York, New York: December 10, 1982). http://www.un.org/Depts/los/convention_agreements/texts/unclos/part5.htm.

and equipment from “dozens” of Vietnamese vessels.⁹⁶ The increase in harassment coincided with China’s annual unilateral fishing ban in sections of the South China Sea, parts of which are disputed by Vietnam.⁹⁷ In June, four Vietnamese fishing boats in waters outside the disputed Spratly Islands reported that Chinese naval ships fired shots into the water near the fishermen’s boats and chased them away.⁹⁸ In July, a Chinese vessel threatened a Vietnamese fishing boat near the disputed Paracel Islands. The Vietnamese fishermen reported that ten armed Chinese “soldiers” boarded their boat, punched and kicked the captain, and confiscated one ton of fish.⁹⁹ These displays of aggression toward fishermen, as well as the cable cutting, fueled unrest in Vietnam and spurred weekend protests against China in Vietnamese cities throughout the summer.¹⁰⁰ Chinese vessels also harassed Philippine fishermen, despite the fact that claimed Philippine waters are not within the jurisdiction of China’s fishing ban. The authorities in Manila claimed that from February to June 2011, Chinese ships had entered into disputed Philippine territory and harassed local fishermen nine times.¹⁰¹

Deployment of patrol ships in the South China Sea—China’s increased assertiveness in disputed waters is attributable in part to a strategic increase in maritime patrols in regions considered especially important or sensitive to China. Responsibility for maritime patrolling is shared by five state agencies and several regional governments.¹⁰² One of these agencies, China’s Bureau of Fisheries, announced in December 2010 that China would strengthen fisheries management in “sensitive” waters, including the South China Sea.¹⁰³ This pledge was put into practice in September 2011 when an additional fisheries patrol ship was sent to waters around the disputed Paracel Islands in order to “strengthen fishery administration in the waters around Xisha [the Paracel Islands], ensure fishery production order and safety of fishermen, and protect China’s sea sovereignty and fishery interest,” according to an Agriculture Ministry official.¹⁰⁴

In June, another agency, China’s State Oceanic Administration, announced that China’s regular maritime surveillance would be strengthened in China’s claimed maritime areas in the South China Sea.¹⁰⁵ China Marine Surveillance, which is the main maritime patrolling body under the State Oceanic Administration, plans to significantly increase personnel and patrol vessels and vehicles in the period during the 12th Five-Year Plan (2011–2015).¹⁰⁶ According to Li Mingjiang, assistant professor at S. Rajaratnam School of International Studies in Singapore, this expansion will enable China Marine Surveillance to conduct daily patrols in areas where it currently has the capacity for only one or two patrols each month.¹⁰⁷

Also in June, the Chinese Maritime Safety Administration ship *Haixun-31* arrived in Singapore on what was noted in the press to be both a goodwill visit and a demonstration of China’s “national rights and sovereignty” in the South China Sea.¹⁰⁸ Singapore does not claim any part of the disputed South China Sea, but one day after *Haixun-31* made its port call, the Singaporean Defense Ministry called on China to clarify its claims in the South China Sea,

saying that ambiguity over China's claimed territory was causing "serious concerns" in the international community.¹⁰⁹

In late August 2011, the *Financial Times* reported on another apparent instance of Chinese patrolling of disputed waters. The newspaper reported that a Chinese warship "confronted" an Indian navy vessel located 45 nautical miles off the Vietnamese coast on July 22. The vessel was returning from a scheduled port call in the southern Vietnamese port of Nha Trang.¹¹⁰ India's Foreign Ministry quickly denied the report, noting only that an unseen caller identifying himself as the "Chinese Navy" contacted the Indian ship, the *INS Airavat*, and stated "you are entering Chinese waters," after which the *INS Airavat* proceeded on its journey. Chinese Foreign Affairs spokesman Ma Zhaoxu said that China had received no diplomatic protest from India over any naval incident.¹¹¹

Military exercises in the South China Sea—China has conducted at least four series of military exercises in the South China Sea since November 2010.¹¹² According to testimony from Jim Thomas, vice president for Studies at the Center for Strategic and Budgetary Assessments, and Stacy Pedrozo, a U.S. Navy captain and military fellow at the Council on Foreign Relations, the PLA Navy conducted several significant exercises in 2010, including a November 2010 amphibious assault exercise that demonstrated PLA Navy capabilities to seize islands and project military power beyond mainland shores.¹¹³ In June 2011, the PLA Navy staged similar drills off the coast of Hainan, China's island province in the South China Sea.¹¹⁴ A PLA exercise took place along the Vietnam-China border in August 2011 as well, fueling media speculation that a large buildup of Chinese troops in the region could be related to South China Sea tensions.¹¹⁵

These exercises demonstrate the modernization of China's naval forces and China's will to project force beyond its shores, developments that have been met with considerable unease in the region. According to Mr. Thomas:

*[T]he stakes in the South China Sea could not be higher. . . . In the last year . . . China has made a series of provocative moves that, when coupled with the continuation of its arms buildup and the development of its naval power projection capabilities, have raised concerns throughout the region about its intentions and potential expansionist designs in the East and South China Seas.*¹¹⁶

Construction on the disputed Spratly Islands, South China Sea—In early June 2011, the Philippines' Department of Foreign Affairs stated that Philippine ships had witnessed a Chinese maritime surveillance vessel and PLA Navy ships unloading building materials and erecting a number of posts and a buoy on Amy Douglas Bank.¹¹⁷ The bank, a small feature in the Spratly Islands, is located within what both China and the Philippines consider their EEZs.¹¹⁸ The 2002 *Declaration on the Conduct of Parties in the South China Sea*, a legally nonbinding agreement between China and the Association of Southeast Asian Nations (ASEAN),* which

* ASEAN is a regional geopolitical and economic organization comprising the Southeast Asian nations of Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore,

provides guidelines for dealing with disputes in the South China Sea, declares that claimants should refrain from occupying previously uninhabited features in disputed areas.¹¹⁹ According to Dr. Storey, if these reports are true, “it would be one of the most serious violations of the 2002 *Declaration of Conduct* to date.” Prior to China’s construction on Amy Douglas Bank, no claimant was proven to have begun construction on unclaimed islands and rocks since the declaration was signed.¹²⁰

Intimidating claimants with harsh rhetoric and closed-door directives—Even during periods of conciliation and cooperation between China and other claimants, Southeast Asian claimants felt pressured to appease China on issues related to maritime disputes, according to officials and experts whom the Commissioners met during a December 2010 trip to Southeast Asia.¹²¹ For instance, Secretary Clinton’s reference to the South China Sea as a “national interest” of the United States during her speech at the 2010 ASEAN Regional Forum was met with mixed reactions in Southeast Asia.† While some regional powers welcomed Secretary Clinton’s speech as reassurance of U.S. commitment to the region, Commissioners were told that her remarks, and China’s adverse reaction to them, prompted some claimant countries to minimize the territorial disputes publicly so as not to attract China’s ire.¹²² For this apparent reason, a joint statement from a U.S.-ASEAN Leaders Meeting in September 2010 in New York City made no mention of the South China Sea, even though an earlier draft of the statement included explicit references to the disputes. According to a Singaporean government official who met with Commissioners, Vietnam’s representative at the New York meeting insisted that all references to the South China Sea be taken out of the statement.¹²³ Commissioners were also told that China had approached all ASEAN members separately and directed them to refrain from discussing the South China Sea, even among themselves.¹²⁴

China’s insistence that claimants not discuss the disputes among themselves was challenged in September 2011, when ASEAN representatives met for two days to discuss a multilateral dispute resolution proposal offered by the Philippines. Senior Philippine diplomats said that Beijing had protested against the meeting, and a Chinese Defense Ministry spokesman remarked shortly after the gathering that China opposes “any move which is designed to multilateralize or internationalize the South China Sea issue.”¹²⁵

Of import, China’s party-run media outlets have published a number of strongly worded editorials advocating that China use its military might to assert its sovereignty over disputed areas in the South China Sea. One such editorial, published in the party-run publication *Global Times*, asserted that China should “punish”

Thailand, and Vietnam. The Official Website of the Association for Southeast Asian Nations, “Overview.” http://www.asean.org/about_ASEAN.html.

† In an address during the 2010 ASEAN Regional Forum, Secretary Clinton asserted that the United States has a strategic interest in the “freedom of navigation, open access to Asia’s maritime commons, and respect for international law in the South China Sea.” She also offered for the United States to play a facilitating role in establishing a binding code of conduct for the claimants. These comments met harsh criticism in China, and China’s Foreign Ministry announced that Secretary Clinton’s remarks were “in effect an attack on China.” U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, DC: U.S. Government Printing Office, 2010), pp. 132–139.

other claimant countries, namely Vietnam and the Philippines, by launching small-scale battles against their forces in the region.¹²⁶

Implications for the United States

China's intensified rhetoric and expanding presence in the South China Sea carry significant implications for the United States. China's growing maritime power could threaten U.S. interests in the Pacific and could lead to Chinese attempts to limit the freedom of navigation that the United States and other countries enjoy in the region. Mr. Thomas testified that as China develops its antiaccess capabilities and becomes increasingly competent operating in its regional maritime environment, China could possibly create a sea denial network stretching from the East China Sea to the South China Sea, eroding the ability of the United States to operate in the region.¹²⁷ (For more information on the PLA's ability to exert control over the western Pacific, see sec. 2 of this chapter.) Such a strategy, according to Captain Pedrozo, aligns with a 1982 Chinese naval maritime plan in which China would replace the United States as the dominant military power in the Pacific and Indian oceans by 2040.¹²⁸ Balbina Hwang, visiting professor at Georgetown University, echoed these concerns in her written testimony to the Commission:

[T]he increasingly assertive Chinese maritime behavior we are witnessing today may be part of a broader strategy to exercise authority over smaller neighbors in the near term by pushing U.S. forces away from its maritime borders to demonstrate rights over the entire South and East China Seas. . . . One necessary concession in China's view will be the reduction of U.S. influence in the region.¹²⁹

Another implication of China's growing assertiveness, especially its harassment and intimidation of foreign vessels, is a growing risk of escalation due to miscommunication and miscalculation between claimants.¹³⁰ Foreign and Chinese analysts agree that China's various maritime enforcement actors often are not sufficiently coordinated with each other.¹³¹ Combined with insufficient mechanisms to report unsafe practices at sea and encourage adherence to international laws and norms, minor incidents could escalate into larger problems. As chances of confrontation grow, issues could be raised for the United States, which has mutual defense obligations with the Philippines and other Asia-Pacific countries including Australia, Japan, New Zealand, South Korea, and Thailand.*

Cyber Issues

In continuation of previous practice, China in 2011 conducted and supported a range of malicious cyber activities.† These included

* For more information on defense obligations between the United States and other countries, see Office of the U.S. Department of State, *Treaties in Force: A List of Treaties and Other International Agreements of the United States In Force on January 1, 2011* (Washington, DC: U.S. Department of State, 2011). <http://www.state.gov/documents/organization/169274.pdf>.

† Recent Commission Reports on the subject include U.S.-China Economic and Security Review Commission, *2009 Annual Report to Congress* (Washington, D.C.: U.S. Government Printing Office, November 2009), chapter 2, section 4; and U.S.-China Economic and Security Review Commission, *2010 Annual Report to Congress* (Washington, D.C.: U.S. Government Printing Office, November 2010), chapter 5.

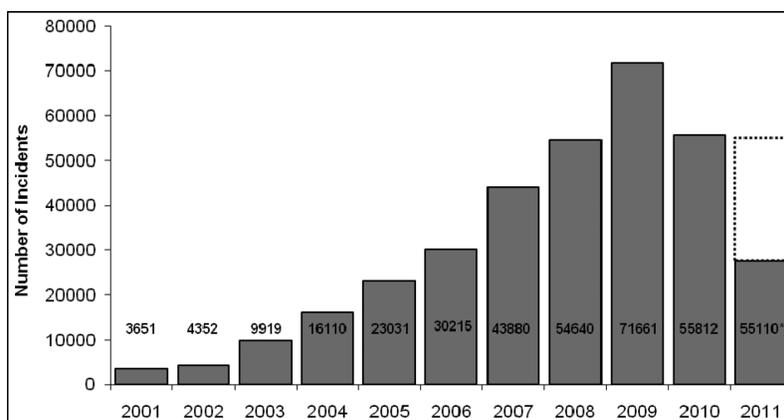
network exploitations to facilitate industrial espionage and the compromise of U.S. and foreign government computer systems. Evidence also surfaced that suggests Chinese state-level involvement in targeted cyber attacks. Expert testimony to the Commission explained and contextualized China's strategy for the use of such attacks to achieve military objectives. In parallel to these developments, China asserted a greater level of control on domestic Internet content and engaged in various online surveillance activities.‡

**Malicious Cyber Activities on
U.S. Department of Defense Networks**

As the Commission reported in 2010, the U.S. government as a whole does not publish comprehensive statistics about malicious cyber activities on its networks. The Commission uses statistics published by the Department of Defense about exploitations and attacks on the department's information systems as one indicator of overall trends in the cybersecurity environment. Figure 2, below, demonstrates changes in the volume of such activities over the past decade. Not all of the incidents depicted below specifically relate to China (the department has not made available that level of detail).

‡ This subsection's findings follow from numerous studies and reports over the past year that implicate China. Many times, investigators attribute incidents on the basis of technical or operational information, the details of which rarely become public. Other times, conclusions rely on inference. In either case, professional investigators typically offer attribution assessments with a specified degree of confidence. Such qualifications sometimes are inadequately conveyed, especially in secondary reports. Moreover, third parties likely use a variety of measures to make their attacks appear as coming from China in order to conceal their identities. (This model is a reasonable explanation for some penetrations, such as those for intellectual property theft, but less so for others, such as those that target Chinese dissidents.) Still, in the aggregate, the developments described below present compelling evidence of Chinese intrusions in practice.

**Malicious Cyber Activities on
U.S. Department of Defense Networks—Continued**
**Figure 2: Department of Defense Reported Incidents of Malicious Cyber
Activity, 2001–2010, with Projection for 2011**



*The figure for 2011 represents a projection based on incidents logged from January 1, 2011, to June 30, 2011. The projection assumes a constant rate of malicious activity throughout the year.

Sources: U.S.-China Economic and Security Review Commission, *Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities*, testimony of Gary McAlum, May 20, 2008; Name withheld (staff member, U.S. Strategic Command), telephone interview with Commission staff, August 28, 2009; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, August 17, 2010; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, September 6, 2011.

Computer network exploitation

In 2011, U.S. and foreign government organizations, defense contractors, commercial entities, and various nongovernmental organizations experienced a substantial volume of network intrusions and attempts with various ties to China. In March, security firm RSA announced that hackers had breached their networks and compromised elements of one of the firm's security products.* Although the company did not name China specifically, subsequent research demonstrated that components of the attack utilized a tool called "HTran," developed by a well-known member of the hacking group "Honker Union of China."† An error in the tool's configuration revealed that the attackers attempted to obscure their location by routing command instructions from mainland China through serv-

*The affected product was "SecurID," a two-factor authentication system where a token generates a unique number that users must provide in order to log into a protected account. Art Coviello, "Open Letter to RSA Customers" (Bedford, MA: RSA, March 17, 2011). <http://www.rsa.com/node.aspx?id=3872>.

†Joe Stewart, "HTran and the Advanced Persistent Threat" (Atlanta, GA: Dell SecureWorks, August 3, 2011). <http://www.secureworks.com/research/threats/htran/>. The tool's developer, Lin Yong, who also goes by the name "Lion," recently announced plans to reconstitute the Hacker Union of China after several years of inactivity. See Owen Fletcher, "Patriotic Chinese Hacking Group Reboots," *Wall Street Journal China Real Time Report*, October 5, 2011. <http://blogs.wsj.com/chinarealtime/2011/10/05/patriotic-chinese-hacking-group-reboots/>.

ers in Japan, Taiwan, Europe, and the United States.‡ The perpetrators then used information about the compromised RSA security product in order to target a number of the firm's customers, including at least three prominent entities within the U.S. defense industrial base. Those intrusions and intrusion attempts, according to some reports, also originated in China and appeared to be state sponsored.¹³²

Many intrusions linked to China involve numerous victims, sometimes spanning sectors and national borders.¹³³ When researchers identify and gain access to elements the systems used to effectuate the intrusion, such as servers that maintain contact with compromised systems, it becomes possible to identify related victims. The breadth of victims itself can suggest state involvement if the diversity in targets exceeds any conceivable scope of interest to a lone, subnational actor (or even a coalition of subnational actors).* Although links to China are speculative and come from secondary reporting, a case study by McAfee, called *Operation Shady RAT* [remote access tool], illustrates this principle.† The 2011 study catalogues a series of penetrations affecting over 70 victim organizations that span numerous sectors, including federal, state, local, and foreign governments; energy and heavy industry; electronics and satellite communications; defense contractors; financial industry; and international sports institutions, think tanks, and nonprofits.¹³⁴ In discussing the possible actors behind the penetrations, the report states:

The [perpetrators'] interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics was particularly intriguing and potentially pointed a finger at a state actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks. The presence of political nonprofits, such as a private western organization focused on promotion of democracy around the globe or a US national security think tank is also quite illuminating. Hacking the United Nations or the Association of Southeast Asian Na-

‡ The tool is probably available from Chinese websites and chat rooms. Whether the servers in mainland China were the true origin of the command traffic can only be verified with cooperation from China Unicom, a Chinese state-owned firm and the relevant network operator. Joe Stewart, "HTTran and the Advanced Persistent Threat" (Atlanta, GA: Dell SecureWorks, August 3, 2011). <http://www.secureworks.com/research/threats/htran/>; and Gregg Keizer, "Researcher follows RSA hacking trail to China," *Computerworld*, August 4, 2011. http://www.computerworld.com/s/article/9218857/Researcher_follows_RSA_hacking_trail_to_China.

* This applies for penetrations that seek to maintain surveillance capabilities or extract information without inherent monetary value. Considerations of target scope do not apply for penetrations targeting personally identifiable or sensitive financial information, along with penetrations that seek to compromise systems for the purposes of creating a botnet.

† For the original report, see Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee: August 2011). <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>. The report itself does not mention China. For suggestions that China may be behind the intrusions, see Ellen Nakashima, "Report on 'Operation Shady RAT' identifies widespread cyber-spying," *Washington Post*, August 3, 2011. http://www.washingtonpost.com/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html; and Mathew J. Schwartz and J. Nicolas Hoover, "China Suspected of Shady RAT Attacks," *InformationWeek*, August 3, 2011. <http://www.informationweek.com/news/security/attacks/231300165>.

*tions (ASEAN) Secretariat is also not likely a motivation of a group interested only in economic gains.*¹³⁵

Cyber penetrations that do not target diverse victims can still indicate state involvement. A February case study, called *Night Dragon*, profiled an exploitation campaign against global companies in the energy and petrochemical sectors. These sectors are of special interest to the Chinese government, which has designated seven “strategic industries” for “absolute state control,” including the power generation and distribution industry, the oil and petrochemicals industry, and the coal industry.¹³⁶ (For more information about China’s strategic industries, see chap. 1, sec. 2, of this Report.) In another indication of institutional involvement, the *Night Dragon* study’s authors noted that:

*[A]ll of the identified data exfiltration activity occurred from Beijing-based IP [intellectual property] addresses and operated inside the victim companies weekdays from 9:00 a.m. to 5:00 p.m. Beijing time, which also suggests that the involved individuals were ‘company men’ working on a regular job, rather than freelance or unprofessional hackers.*¹³⁷

While the study’s authors could not definitely identify the perpetrators, an opaque web-hosting company and its Shandong-based operator appeared to be involved.¹³⁸ As described below, Shandong Province is connected to several other penetrations over the past several years.

China-based hackers increasingly use indirect approaches to gain access to sensitive information systems. In June, Google announced that it had discovered a widespread but targeted “phishing” campaign that had compromised Google Mail (Gmail) accounts.* The company disclosed that:

*This campaign, which appears to originate from Jinan, China, affected what seem to be the personal Gmail accounts of hundreds of users including, among others, senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists.*¹³⁹

Aside from Gmail users, the campaign reportedly affected certain U.S. government e-mail accounts at the Department of State, the Department of Defense, and the Defense Intelligence Agency. The perpetrators leveraged access to compromised accounts to perpetuate the campaign by spreading malicious software to the victims’ contacts.† As the Commission reported in 2009, Jinan, Shandong Province, is the home of one of China’s Technical Reconnaissance

*“Phishing” is “an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent web site that appears legitimate. The user then may be asked to provide personal information such as account usernames and passwords that can further expose them to future compromises. Additionally, these fraudulent web sites may contain malicious code.” U.S. Computer Emergency Readiness Team (U.S.-CERT), “Report Phishing.” http://www.us-cert.gov/nav/report_phishing.html.

† This is called the “man-in-the-mailbox” technique. John Markoff and David Barboza, “F.B.I. to Investigate Gmail Attacks Said to Come From China,” *New York Times*, June 2, 2011. http://www.nytimes.com/2011/06/03/technology/03google.html?_r=1.

Bureaus. These entities serve as a computer network exploitation arm for the Third Department of the PLA's General Staff Department, which collects signals intelligence.¹⁴⁰ A vocational school linked to the December 2009 Google penetration is also located in Jinan.¹⁴¹

During a Commission trip to China in August 2011, representatives of foreign businesses that operate in China placed computer network intrusions alongside mandated technology transfers and invasive technical standards inspection schemes as the most serious threats to their intellectual property. Chinese efforts suggest that, for firms without a physical presence in China, computer network intrusions may pose the most serious threat to intellectual property.

Computer network attack

Along with the considerable computer network exploitation capabilities described above, the Chinese government has computer network attack capabilities. As the Department of Defense's 2011 annual report to Congress on *Military and Security Developments Involving the People's Republic of China* states, "[t]he PLA has established information warfare units to develop viruses to attack enemy computer systems and networks."^{*} This has implications for military and nonmilitary targets. For example, a 2011 global survey of critical infrastructure operators conducted by McAfee and the Center for Strategic and International Studies identified government-sponsored sabotage as a central cyber threat. The plurality of respondents, 30 percent, identified the Chinese government as the greatest concern.¹⁴² While the survey measured perceptions rather than events, its findings illustrate the concerns of those on the "frontlines" of infrastructure protection.[†]

Perhaps the most compelling evidence that surfaced in 2011 linking the Chinese government to cyber attacks was a July documentary presented on China Central Television 7 (CCTV-7), the government's military and agricultural channel. A brief segment demonstrated what appears to be a PLA "point and click" distributed denial of service attack launched against a Falun Gong-related website hosted on a network at the University of Alabama in Birmingham. Based on Internet Protocol data exposed in the program and information from the school's network administrators, the attack appears to have taken place in 2001 or earlier.[‡] According to the footage, the PLA's Electrical Engineering University developed the software used to launch the attack.¹⁴³ Some reports about this

^{*}Parallel developments include "tactics and measures to protect friendly computer systems and networks." Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011* (Washington, DC: Department of Defense, 2011), p. 37.

[†]China also faces challenges in securing infrastructure. For example, see Paul Roberts, "Glass Dragon: China's Cyber Offense Obscures Woeful Defense," *Threatpost*, April 27, 2011. http://threatpost.com/en_us/blogs/glass-dragon-chinas-cyber-offense-obscures-woeful-defense-042711. See also Jim Finkle, "Exclusive: China software bug makes infrastructure vulnerable," Reuters, June 16, 2011. <http://www.reuters.com/article/2011/06/17/us-cybersecurity-china-idUSTRE75G0CV20110617>.

[‡]Other attacks have been documented more recently, including in 2011. See, for example, Benjamin Joffe-Walt, "U.S. Congresswoman Condemns Chinese Attack on Change.org," *Change.org Blog*, April 26, 2011. <http://blog.change.org/2011/04/u-s-congresswoman-condemns-chinese-attack-on-change-org/>.

incident suggested that the attack shown was rudimentary, apparently on the basis of the program's graphical user interface and the attack method itself. However, the scope and implications of the attack cannot be determined from the footage.* Initially posted on the broadcaster's website, the documentary episode was promptly removed by CCTV when international media started to report the story. This measure, along with the offhanded manner by which the show presented the material, led most reports to characterize the footage as an accidental disclosure.¹⁴⁴

Military strategies

Like the United States and other nations with modern militaries, China seeks to leverage cyber capabilities to achieve or help achieve military objectives. As the Department of Defense's 2011 annual report to Congress on *Military and Security Developments Involving the People's Republic of China* states, China's military could use cyber warfare "to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities."¹⁴⁵ Expert testimony to the Commission in 2011 provided details about how China would seek to employ such techniques. David A. Deptula, a retired U.S. Air Force lieutenant general, testified that China has "identified the U.S. military's reliance on information systems as a significant vulnerability that, if successfully exploited, could paralyze or degrade U.S. forces to such an extent that victory could be achieved."¹⁴⁶ Specifically, General Deptula categorized cyber attacks on U.S. C4ISR [command, control, communications, computers, intelligence, surveillance, and reconnaissance] assets as a key action that China's military would take "to impede U.S. military access to the Asian theater in the event of a U.S.- China conflict."¹⁴⁷

Martin C. Libicki, senior management scientist at the RAND Corporation, testified that operational cyber attacks, such as those that would degrade U.S. logistics systems, present a serious challenge to U.S. military forces. As such, the "[U.S.] Department of Defense needs to take the prospect of *operational* cyberwar seriously enough to understand imaginatively and in great detail how it would carry out its missions in the face of a full-fledged attack" (emphasis in original).¹⁴⁸ He characterized *strategic* cyberwar, such as "a cyberattack on the U.S. power grid, throwing the Midwest into the dark," as less likely in the context of a Taiwan contingency, a conceivable backdrop to hostilities between the United States and China. Because China's leadership would likely seek to keep the United States out of such a contingency, a strategic cyber attack on the United States might have the opposite effect and could therefore serve as a "very poor coercive tool."¹⁴⁹ However, this assessment may not hold for other types of contingencies.

*A graphical user interface could easily be mated with a controller capable of launching a significant distributed denial of service attack. A military organization would likely use such an interface in order to make its computer network operations tool more accessible to its force. With respect to the method of attack itself, computer security experts generally regard distributed denial of service attacks as one of the more manageable threats. However, certain techniques are sophisticated and difficult to mitigate. For a brief discussion of what constitutes a significant distributed denial of service attack, see Craig Labovitz, "The Internet Goes to War" (Chelmsford, MA: Arbor Networks, December 14, 2010). <http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/>.

Surveillance and censorship

The Chinese government asserted a greater level of control over domestic Internet access and content in 2011. In May, it created a new State Council-level entity to centralize “online content management,” a euphemism in China for various forms of regulation and censorship.¹⁵⁰ More recently, China’s censors blocked web-based speculation by Chinese citizens about the health and possible death of former Chinese President Jiang Zemin following his failure to appear at a celebration of the 90th anniversary of the CCP’s founding.¹⁵¹ This year’s social media-assisted demonstrations in the Arab world, sometimes leading to regime change, appear to have intensified the Chinese government’s traditional apprehension about political discourse.¹⁵²

Other new measures appear to be technical outgrowths of existing policies. Fang Binxing, the creator of China’s “great firewall,” acknowledged in February that he personally used six virtual private networks to test whether they could overcome China’s traffic-blocking measures.¹⁵³ Subsequently, several times throughout 2011, new Chinese censorship measures disrupted this previously reliable method used to circumvent local restrictions on overseas web content.¹⁵⁴ Chinese authorities also curtailed domestic web content. The Chinese Academy of Social Sciences announced in July that the government shuttered 1.3 million websites throughout 2010.¹⁵⁵ Some percentage of these sites probably hosted malicious software as opposed to content deemed undesirable to the Chinese government (such as pornography or political speech), but the government does not make available figures with that level of specificity.

In at least one instance this year, U.S. Internet traffic improperly transited Chinese networks.¹⁵⁶ Following a series of similar incidents documented in the Commission’s 2010 Annual Report, select U.S.-generated Internet traffic from social networking site Facebook travelled on a route through Chinese state-owned telecommunications firm China Telecom on March 22, 2011.* The exact path of the diversion could not be reconstructed, but the affected traffic may have traversed networks physically located in China.† Although perhaps accidental, such an incident demonstrates a vulnerability that could be used for exploitation or attack. The capability to initiate or exploit erroneous traffic routes exists for all Internet Service Providers, but state ownership of the entire sector in China (as another “strategic industry”) elevates the risk of systemic abuse, either as an intentional measure directed against external Internet users or a side effect of internal censorship policies.

Implications for the United States

China appears to use computer network exploitations to conduct espionage against governments and military entities, commercial entities, and nongovernmental organizations. In parallel, the PLA maintains capabilities to execute computer network attacks. These

*The data also traversed Hanaro Telecom South Korea’s networks.

†Alternatively, the data could have traversed China Telecom networks physically located in North America. BGPmon.net, Untitled, March 26, 2011. <http://bgpmon.net/blog/?p=499>.

practices have myriad implications for the United States. Computer network exploitation directed against government entities jeopardizes their ability to handle sensitive information securely and reliably. Network exploitations and attacks on military entities may compromise large-scale weapons systems, delay deployments, or cause a number of other events that harm U.S. national security and regional stability in Asia. China's exploitations that compromise commercial entities' proprietary information and intellectual property likely bolster Chinese firms' capabilities and erode U.S. businesses' remaining technological advantages. In addition, Chinese penetrations of, and assaults on, nongovernmental organizations' networks complicate their operations and could pose security risks for their members and affiliates.

Conclusions

- Over the past year, China has demonstrated progress in modernizing the PLA. Recent developments confirm that the PLA seeks to improve its capacity to project force throughout the region.
- Continued improvements in China's civil aviation capabilities, as first noted in the Commission's 2010 Annual Report, enhance Chinese military aviation capabilities because of the close integration of China's commercial and military aviation sectors.
- In an effort to calm regional fears, China attempts to broadcast a benign image of its growing military capabilities. Official statements from Beijing over the past year describe China as a status quo power and downplay its military modernization efforts.
- In 2011, China continued a pattern of provocation in disputed areas of the South China Sea. China's policy in the region appears driven by a desire to intimidate rather than cooperate. Many of China's activities in the region may constitute violations of the *United Nations Convention on the Law of the Sea* and the *Declaration on the Conduct of Parties in the South China Sea*. While China sometimes demonstrates a willingness to cooperate with other claimants to disputed waters in the South China Sea, it is unlikely that China will concede any of its claims.
- China's government or military appeared to sponsor numerous computer network intrusions throughout 2011. Additional evidence also surfaced over the past year that the Chinese military engages in computer network attacks. These developments are consistent with the PLA's known missions and organizational features, as noted by the Commission's *2009 Annual Report to Congress* and contracted research study *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*.*
- China's military strategy envisions the use of computer network exploitation and attack against adversaries, including the United States. These efforts are likely to focus on operational systems, such as command, control, communications, computers, intel-

*This report was prepared for the Commission by Northrop Grumman and is available on the Commission's website at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

ligence, surveillance, and reconnaissance assets. This could critically disrupt the U.S. military's ability to deploy and operate during a military contingency. Chinese cyber attacks against strategic targets, such as critical infrastructure, are also possible.