Prepared Statement of
Mark A. Stokes
Executive Director
Project 2049 Institute
Before
The U.S.-China Economic and Security Review Commission

Hearing on China's Military Modernization and its Implications for the United States
Thursday, January 30, 2014
Room 2118, Rayburn House Office Building

Mr. Chairman and members of the commission, thank you for the opportunity to participate in today's hearing on a topic that is important to U.S. interests in peace and stability in the Asia-Pacific region. It is an honor to testify here today.

The Chinese Communist Party (CCP) and the People's Liberation Army (PLA) are steadily advancing their capacity to exercise coercive military power in order to advance national security interests. Increasingly less constrained by technological barriers that have hampered it in the past, the PLA has been investing in capabilities that may offset shortcomings in the face of a more technologically advanced adversary.

My presentation today focuses on three aspects of the PLA's broad force modernization program -- command, control, communications, computer, intelligence, surveillance, and reconnaissance (C^4ISR); computer network operations (CNO), and counterspace. Looking horizontally beyond its immediate periphery and vertically into space, Chinese analysts view disruption of the U.S. ability to project conventional power to support alliance obligations and legal requirements under the Taiwan Relations Act (TRA) as a legitimate force modernization goal. These three areas function as critical enablers for military use of force.

As a preface, PLA military modernization should be viewed within a political context. Military modernization and political warfare have a symbiotic relationship. Political warfare adopts active measures to promote the rise of CCP legitimacy within a new international order and defend against perceived threats to state security. Political warfare employs strategic psychological operations and propaganda as means of influencing international discourse and policies of friends and potential foes alike. Political warfare, carried out both during peacetime and in armed conflict, amplifies or attenuates the political effects of military instrument of national power. For example, coercive persuasion, which integrates demonstrated or latent military capabilities with political warfare, is intended create the conditions for resolution of cross-Strait differences on Beijing's terms.

The objects of political warfare and military coercion have extended beyond Taiwan. To support broader political goals, the PLA is gradually transforming into a modern military force capable of responding to an increasingly diverse set of contingencies further from its shores. National pride resulting from successes in the information, cyber, and space domains shores up domestic CCP legitimacy. Advances in military capabilities also encourage greater risk in enforcing territorial claims in the East and South China Seas. However, the priority remains a credible capacity to exercise decisive use of force to coerce the Republic of China (Taiwan) into a negotiated solution on Beijing's terms and discourage foreign intervention. As time goes on, the same political-military capabilities that could be exercised against Taiwan could be applied toward other disputes around the PRC's periphery.

C^4ISR

With the foregoing in mind, development of a survivable and responsive C^4ISR system is a central PLA force modernization priority. C^4ISR systems reduce surprise, increase warning time, facilitate the sharing of information within an often stovepiped PLA bureaucracy, ensure continuity of operations, and allow senior decision makers to make better-informed decisions. Although hardware is important in times of emergency, weapon systems are of limited utility without an advanced C^4ISR system.

Information technology is at the heart of C^4ISR, an area in which the PLA has traditionally been at a relative disadvantage. Today's global information revolution is a phenomenon that is transforming the world's industrial-based societies and economies. In our everyday lives, we look to information and communications technology to work, function, cooperate, and compete more effectively. The trend towards increased computing power to process, collate, and analyze a vast quantity of sensor data in order to mitigate and respond to a range of security challenges has turned the information revolution into a C^4ISR revolution. Success or failure in PLA use of force is likely contingent upon the quality of information available to commanders and the manner in which it is used.

Command and Control

The PLA is enhancing its ability to command and control forces that could be brought to bear in a future contingency. The CMC's peacetime conventional command and control system is centered today upon the General Staff Department (GSD), three other first level general departments -- General Political Department (GPD), General Logistics Department (GLD), and General Armaments Department (GAD – seven military regions, PLA Navy, PLA Air Force (PLAAF), and Second Artillery Force.

In a crisis situation, the CMC's peacetime command and control of conventional forces likely would transition to a joint task force structure, referred to as a Joint Theater Command (JTC). The form and substance of a contingency JTC appears to be flexible and scenario dependent.

In a notional scenario, a CMC vice chairman, CMC member, and/or senior GSD and GPD authorities (eg, Deputy Chief of the General Staff and GPD deputy director) could serve as JTC commander and political commissar. Under CMC guidance, GSD likely would the principle organization responsible for overseeing the transition from peace to wartime command and control. A JTC staff could be centered upon the most relevant military region(s), with additional elements drawn from GSD, the other three general departments, and representatives from the Air Force, Navy, and Second Artillery. The primary mission of the JTC would be to plan and prepare for joint operations and exercise authority over national level PLA assets and corps-level components assigned to the JTC. The CMC, GPD, and joint theater political authorities would also oversee the transition of political warfare assets from peacetime to a wartime status.

The CMC likely would likely augment forces within a military region through apportionment of selected assets from throughout the PLA to the JTF and corps-level Navy, Air Force, and conventional Second Artillery component commands. Direct CMC oversight of and integration with the JTC ensures an orchestrated political-military strategy with access to party and state resources. The GSD Operations Department (also known as the GSD First Department), one of 12 subordinate second-level GSD departments, manages the National Joint Operational Command Center and oversees a specialized contingency office to coordinate with civilian authorities during emergencies.

JTC employment of national assets likely would be carried out via a primary JTC command center. The primary command center would be supported by reserve and rear command posts, and if necessary, a forward command post. The forward command post and the rear command post, which is responsible for logistics support, reports to the primary command center. The reserve post would assume duties as the primary command center if the latter is neutralized.

PLA writings indicate that the JTC's primary command and control center would be comprised of a subordinate communications center, firepower coordination center, intelligence information center, an information operations (IO) or electronic countermeasures (ECM) command center, and an operations support center responsible for meteorological and other functions. Representatives from the Navy, Air Force, and conventional Second Artillery component command likely would maintain coordination cells within the JTC command center.

Second Artillery, Air Force, and Navy component commands under the JTC would coordinate long range precision strike operations through the firepower coordination center. PLA analysts view an air campaign as an integral component of "joint firepower warfare" operations involving the coordinated use of PLAAF strike aviation assets and Second Artillery conventional theater missiles. An intelligence information center theoretically would integrate and distribute sensor data, navigation, survey, mapping, and weather information. The command and control system reportedly allows for skip echelon communication from the battalion/regimental level and up. Joint IO/ECM center responsibilities may include oversight of collection and analysis of electronic reconnaissance, development of an ECM concept of operations and electronic attack plan; assignment of responsibilities and targets, transmission of orders to ECM units; and coordination with the JTF leadership and other centers.

Nuclear and conventional command and control systems appear to be managed separately in both peacetime and wartime. The CMC likely would retain strict control over nuclear weapons in a crisis situation, rather than apportioning to JTC authority. This issue warrants further study.

Communications and Computers

In a crisis situation, the PLA's peacetime and national civilian telecommunications infrastructure would transition to meet JTF requirements. To support operations at increasing distances from Chinese shores, the PLA is investing heavily into advanced information and communications technology. JTF communications authorities, most likely overseen by the GSD Informatization Department, would leverage military and national civilian telecommunications infrastructure as needed to establish a joint operational command communications network to support the command structure. JTF communications centers likely would include representatives from the general departments, Navy, Air Force, and Second Artillery and as well as provincial telecommunications offices.

The GSD Informatization Department is responsible for developing, constructing, operating, and maintaining a PLA-wide interoperable joint command and control communications system. Priorities include development and fielding of a capability - an Integrated Command Platform -- that correlates sensor data produced by GSD assets and distributes to joint and corps-level component commanders. Sensor data produced by corps-level component units likely would contribute to a common operational picture. In addition, Navy, Air Force, and conventional Second Artillery units maintain independent communication systems in peacetime that likely would be interoperable with a JTF in a crisis situation. The CMC likely maintains a separate communications network reserved for nuclear command and control.

At the tactical level, the PLA appears to be applying principles of network centric warfare to communicate and correlate data from increasingly sophisticated sensor architecture. Network-centric warfare equips soldiers, airmen, and sailors with a common operational and tactical picture that could significantly increase situational awareness. As a result, individuals and units equipped to participate in the network could synchronize actions without necessarily having to wait for orders, which in turn reduces their reaction time. In addition, a tactical network may allow for dispersed and flexible operations at lower cost. Therefore, the introduction of a networked common tactical picture, based on an advanced tactical data link program, could be a paradigm shift that could gradually break down the PLA's traditionally stovepiped approach to defense. The effectiveness of such a system may depend upon the level of political control imposed on tactical commanders and trust in individual operators.

In addition to static infrastructure of fiber optic cables, line of sight microwave and tactical radios, the PLA has been investing in the development and production of dedicated military communications satellites. Broadband satellite communications enable transmission of high volumes of data from sensors to a wide variety of users at increasingly extended ranges from China's periphery.

Intelligence, Surveillance, and Reconnaissance

The PLA's C^4ISR systems also includes ISR assets that would support operations against targets operating in the land, maritime, and space domains. The PLA's ability to strike mobile targets is likely bounded by the range of its persistent surveillance. To expand its battlespace awareness, the PLA is investing in space-based, airborne, and surface-based sensors that could enable monitoring of military activities in the Western Pacific, South China Sea, and Indian Ocean.

The PLA manages increasingly sophisticated space-based electro-optical (EO), synthetic aperture radar (SAR), and electronic reconnaissance (ELINT) satellites. Space-based systems expand the PLA's battlespace awareness and support strike operations further from Chinese shores. The GSD Intelligence Department most likely drives requirements and leverages the data produced by space-based sensors. Space assets enable the monitoring of naval activities in surrounding waters and the tracking of air force deployments into the region. A constellation of small electronic reconnaissance satellites, operating in tandem with SAR satellites, could provide commanders with precise and timely geolocation data on mobile targets. Space-based sensors also provide images necessary for mission planning functions, such as navigation and terminal guidance for land attack cruise missiles, including automated target recognition technology that correlates pre-loaded optical, radar, or infrared images on a missile system's computer with real time images acquired in flight.

Satellite communications also offer a survivable means of linking sensors to strike systems, and will become particularly relevant as PLA interests expand further from Chinese shores. Existing and future data relay satellites and other beyond line of sight communications systems could relay targeting data to and from the JTC and corps-level component command centers. Authors publishing in authoritative journals have advocated accelerating and expanding China's space-based surveillance system to cover targets operating out to a range of 3000 kilometers from the shoreline. Increasingly greater spatial resolution and an ability to monitor U.S. activity in the Asia-Pacific region (including the locations of US aircraft carrier battle groups) in all weather conditions are likely to enhance China's ability to conduct military operations farther from shore.

In a crisis situation, China may have the option of augmenting existing space-based assets with microsatellites launched on solid-fueled launch vehicles. Weighing between 10 and 100 kg, microsatellite programs to date appear experimental in nature, but competency and experience could translate into a lower cost, operationally responsive space capability.

Airborne ISR assets include increasingly advanced and diverse range of unmanned aerial vehicles (UAVs) operated by GSD, Navy, Air Force, and Second Artillery. The Air Force and Navy also operate manned peacetime aerial reconnaissance aircraft. Beyond satellites and airborne ISR platforms, the PLA appears to be assessing the feasibility of "near space" flight vehicles equipped with EO, SAR, and ELINT sensors. Near space flight vehicles, operating at the upper extremes of the atmosphere, may emerge as a dominant platform for a persistent regional wide surveillance capability over the next decade. Coverage from platforms similar to satellites in low earth orbit could offer significant improvements in resolution. Duration of flight for near space vehicles far exceeds that of UAVs and their small radar and thermal cross-sections make them difficult to track and target.

In addition to space-based, near space, and airborne sensors, PLAAF radar brigades comprise a large air surveillance network, including at least one over the horizon (OTH) "skywave" radar system that monitors air and maritime activity out to 3000 kilometers.

In a contingency situation, sensor data from a range of platforms likely would be correlated or fused within a JTC intelligence information center, which would staffed in part by apportioned assets from GSD Intelligence (Second) and perhaps Technical Reconnaissance (Third) Departments. Theoretically, the center could task satellites and airborne platforms and other collection assets, analyze information, and ensure a JTC leadership maintains situational awareness.

Computer Network Operations

The PLA oversees a large CNO infrastructure that functions as an integral component of its C^4ISR system. Computer networks are the main arteries of cyber operations. Information and communications technology enable and enhance the capabilities of actors to engage in the cyber realm. Modern societies and governments increasingly rely on cyber-based information systems in order to process, coordinate, and manage critical processes necessary to function. Yet due to the highly automated and interconnected nature of economic transactions and the protection of critical infrastructure, the cyber domain is emerging as a new dimension in conflicts of the future. The PLA's investment into CNO capabilities represents a significant evolution in the PRC's quest for total information awareness.

CNO can be viewed in the context of *informatization,* which is a means to ensure sustained economic growth, compete globally in the information technology realm, and ensure national security. Informatization relies on information security systems that can support economic restructuring and national security. In the information age, information security within the broadest context as ensuring CCP legitimacy, enhancing the party-state's ability to consolidate power, defending national networks against internal and external threats, and supporting economic development. Security of the party and state requires mastery of the global cyber sphere.

In the military context, CNO often is referred to as "network attack and defense," based on the premise that "without understanding how to attack, one will not know how to defend." In the U.S. lexicon, CNO includes computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). Cyberspace is an important domain for national security, and CNO is viewed as a critical enabler for ensuring future operational effectiveness.

CNO capabilities could be brought to bear in peacetime and in a crisis situation. The GSD Technical Department (also known as the GSD Third Department) has cognizance over a vast signals intelligence and CNO infrastructure. These functions are encompassed within the euphemism of "technical reconnaissance," which is a foundation of "informatized" warfare. GSD Third Department command authorities manage a complex CNE, or cyber reconnaissance, infrastructure that exploits vulnerable computer networks around the world, while also ensuring the integrity of classified networks within China. The Third Department Second Bureau, headquartered in Shanghai, is an illustrative example of a front end collection and analysis entity. Cyber reconnaissance builds upon a traditional core competency in SIGINT, advanced high performance computing and encryption/decryption technical capabilities, and a status as China's largest employer of well-trained linguists. Faced with its own challenges to communication systems and computer networks, the Third Department has responsibility for assuring the security of PLA computer systems in order to prevent foreign adversaries from gaining access to sensitive national security information.

Operational Third Department entities operate alongside technical reconnaissance bureaus under military regions. While unclear, entities engaged in CNO likely are fragmented and stovepiped.

Information security engineering bases in Shanghai, Beijing, and Tianjin serve as windows to the broader academic and commercial cybersecurity community.

Which organization within the PLA has responsibility for CNA remains an open question. Most assessments point toward the GSD Fourth Department, which traditionally has been the principle staff organization responsible for radar-related planning and electronic countermeasure (ECM) operations. A preliminary survey reveals few clues about a Fourth Department strategic cyber attack mission. GSD Third Department itself and PLA Second Artillery Force, China's answer to U.S. Strategic Command, are alternate candidates. In general, the organizational structure for strategic cyber attack requires greater attention.

Cyber espionage and potential disruption of critical U.S. computer networks have emerged as a significant national security challenge. In his May 2011 *International Strategy for Cyberspace*, President Obama declared that the United States will work with partners to "encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate." In response, the U.S. national security community is adopting a multifaceted approach to address the cybersecurity challenge, including through strengthened awareness, deterrence, greater investment into counterintelligence, and international partnerships with defense establishments familiar with PLA cyber operations, such as Taiwan. Counterintelligence tools include both disruption and deception, which offset the inherent asymmetric advantages that the attacking side enjoys.

The PLA's ambitious cyber operations also warrant consideration of appropriate responses to hostile cyber network attacks intended to neutralize U.S. command and control and critical infrastructure. Most important would be the determination of what types of computer network attacks would constitute an act of war, and what types of responses would be most appropriate.

Counterspace

In addition to C^4ISR and cyber warfare, counterspace operations is another priority area for PLA force modernization. Freedom of action in space, and an ability to deny an adversary access to its space assets, offer military advantages in land, air, maritime, and information domains. The United States and other powers are dependent on space assets for military operations and to ensure an advantage over potential adversaries. The U.S. relies on space-based assets for communications, navigation, missile warning, environmental monitoring, and reconnaissance. Given vulnerabilities in space infrastructure, a potential adversary could target U.S. space assets and seek to deny advantages gained through the leveraging of space capabilities. Space superiority is characterized by the freedom to operate in space while denying the same to an adversary.

Policymakers in Beijing view space power as one aspect of a broad international competition in comprehensive national strength and science and technology (S&T). The PLA has been investing in a range of passive and active counterspace technologies, and has demonstrated a rudimentary capability to track and intercept satellites orbiting around the earth's poles. The ability to engage targets in space is viewed as part of a broader effort to field a "national aerospace security system." Chinese writings tend to link counterspace with an ability to track and engage all flight vehicles transiting space, including ballistic missiles. China's space and missile industry conducted successful tests of a kinetic kill vehicle in January 2007 and January 2010, thus demonstrating a basic ability to intercept polar orbiting satellites and medium range ballistic missiles during the mid-course of flight.

Chinese pundits highlight trends toward militarization of space and outline requirements for counterspace operations in future conflicts. However, non-destructive means of denying an enemy use of satellites and mitigating threats from space debris may be a more urgent priority than fielding kinetic kill vehicles. As noted by one former U.S. national intelligence authority, "counter-command, control, and sensor systems, to include communications satellite jammers, are among Beijing's highest military priorities."

Elements of a viable counterspace program include an architecture that fuses multiple sources of data in order to detect, identify, and track satellites and other space objects; development and production of technologies that neutralize threats; and a clearly defined and well trained organization able to coordinate and execute counterspace operations. Counterspace operations depend upon a survivable space surveillance network, and China is gradually developing a supporting infrastructure. China's ability to track and mitigate space debris could serve as a metric for the amount of progress that is being made.

The lead organization within the PLA for counterspace operations remains an open question, as does the relationship between national space and counterspace policies and programs. GAD-affiliated organizations have produced assessments of space strategy, characterizing space power and advocating prioritization of space technology in order to further PLA warfighting under conditions of "informatization," including counterspace operations and "space superiority." Analysts differentiate between "hard" and "soft" counterspace measures, and relevance of an independent "space force" that would centralize space operations under a unified command.

Discussion of an independent space force has been underway since the 1990s, and resolution of the issue has yet to clear. While GAD manages a space launch, tracking, and control network, both the PLAAF and Second Artillery have indicated intent to establish space operations as a core competency. The PLAAF argues that battlespace for air defense operations should be extended beyond the atmosphere and into space and over sea, yet integrated under a single air defense command organization. Under an ambitious and long term force development concept of "integrated air and space (aerospace) operations," one PLAAF analyst has argued that "space control is a reasonable extension of air control."

At the same time, the Second Artillery has argued that it should be responsible for military space operations. For example, an internal Second Artillery text references a "Second Artillery space operations unit" as an operational support function. However, no clear operational infrastructure for a space mission is evident in Second Artillery order of battle. Theoretically, existing medium, intermediate, and intercontinental ballistic missiles could be adapted for a space intercept role by reprogramming missile guidance and fusing.

One analysis explains that the space domain would be divided along the Karman Line: the PLAAF would assume the air defense mission for threats below 100 km, while the Second Artillery would be responsible for threats above 100 km. A senior PLAAF Equipment Department authority noted the service's investment into missile defense development. Regardless, uncertainty surrounds the role of the GAD, PLAAF, Second Artillery, or other entities in managing space operations, including planning, programming, and budgeting functions; satellite launch, tracking, and control; ground processing; and counter-space operations.

Beyond the issue of space control, the PLA has been investing in a wide range of passive and active means to deny a potential adversary's ability to leverage space-based assets. R&D investments include foreign satellite communications monitoring systems, electronic countermeasure systems to disrupt an opponent's use of space-based systems, as well as developing the capability for physical destruction of satellites in orbit. The PLA and civilian counterparts also have been enhancing national satellite laser range finding capabilities, and investing in radar systems for satellite surveillance and tracking. China also is investing into the means to deny an adversary effective use of space-based ISR assets through concealment, camouflage, and deception.

Conclusion

Senior authorities in Beijing seek to reshape the global order in a manner consistent with the interests of the Chinese Communist Party. Economic, cultural, political and military power, guided by political-military concepts such as the "Three Warfares," are critical for expanding and strengthening Beijing's global influence and mitigating domestic challenges to the party's monopoly on power.

Despite heightened tensions in the East and South China Seas, the subordination of ROC to CCP authority remains the principle driver for PLA force modernization. Diminished *military* tensions across the Taiwan Strait today should not mask the fundamental instabilities simmering beneath the surface. Political warfare operations, backed by a large conventional missile infrastructure in southeast China, are growing in intensity and scope. The subordination of Taiwan, and its democratic system of government, to PRC authority under a "One Country, Two Systems" formula remains the CCP's most urgent core interest. The objective reality is that Taiwan, under its current ROC constitutional framework, exists as an independent, sovereign state. The two equally legitimate governments – the PRC and ROC – are currently committed to One China principles, under which they exercise exclusive administrative jurisdiction over the territory under their respective control, with neither side subordinate to the other. In the context of the U.S. "One China" policy, a "One China, Two Governments" framework may serve as the most accurate representation of the status quo in the Taiwan Strait.

However, from Beijing's perspective, Taiwan's democratic government – an alternative to mainland China's authoritarian model – presents an existential challenge to the CCP's monopoly on domestic political power. With political legitimacy in the Taiwan Strait viewed as a zero sum game, authorities in Beijing have long sought the political subordination of Taiwan under a "One Country, Two Systems" principle. The resolution of cross-Strait differences is constrained without broad acknowledgement if not recognition of the ROC's political legitimacy within the international community.

Actual, presumed, or latent capabilities, amplified by an equally capable political warfare infrastructure, increases the PLA's capacity for coercive persuasion in resolving sovereignty and territorial disputes in the CCP's favor. Growing military capabilities – real or perceived – are intended to achieve near term political effects, including effecting change in U.S. policy toward Taiwan and the region as a whole. As its persistent sensor and command and control architecture increases in sophistication and range, the PLA's ability to hold at risk an expanding number of targets throughout the western Pacific Ocean, South China Sea, and elsewhere around its periphery is expected to grow. A survivable space-based sensor architecture, able to transmit reconnaissance data to ground sites in China in near-real time, facilitates the PLA's ability to project firepower at greater distances and with growing lethality and speed.

The PLA's development of counterspace, cyber, and C4ISR capabilities could affect the relative balance of power in Asia. U.S. satellites and computer networks may be vulnerable to disruption during a crisis. However, the degree of vulnerability depends upon the types of investments that DoD makes to defend assets in space and computer networks over the next 5-10 years. The relative balance of power also depends on vulnerabilities in the PLA's command, control, and communications system, and the willingness of the United States and its security partners to exploit those vulnerabilities in a crisis situation. The balance of power also depends on a balance of political will and adherence to enduring principles that have guided American foreign policy for decades.

Finally, concepts associated with Air Sea Battle and Offshore Control both have merits. Deterring PRC resort to use of force to resolve sovereignty and territorial disputes requires a demonstrated capacity to deny the PLA its military objectives. The ability to exploit vulnerabilities in the PLA's command and control system, even one that could be held in reserve, should be a top priority. In a crisis, the national command authority should have a range of options from which to choose, bearing in mind escalatory risks associated with each option. A unilateral declaratory policy that limits U.S. military action to offshore control, with no parallel reduction in the most destabilizing aspects of PLA force modernization (eg., conventional ground-based ballistic and land attack cruise missiles), may only encourage greater risk in Beijing's approach to resolving disputes in the region.

END