Prepared Statement before the U.S.-China Economic and Security Review Commission

Hearing on "China in Space: A Strategic Competition?"

April 25, 2019

Jonathan S. Ray
Research Director
Special Programs Division
SOS International LLC

I would like to thank Chairman Bartholomew, Commissioner McDevitt, and other members of the Commission for inviting me to speak today. It is an honor to be invited back.

My testimony focuses on the PLA's strategy and activities in the space and network (or cyber[1]) domains, and their implications for strategic competition between the United States and China in those domains. To me the top issues for strategic planners and policymakers are:

- China's holistic view of the space, network, and electromagnetic domains as part of a broader information domain;
- An aggressive military doctrine for China to use network attack methods against U.S. space assets in steady state and early in any conflict; and
- The implications and challenges posed by the creation of the Strategic Support Force (SSF).

I conclude with recommendations for Congress that prioritize constant monitoring of Chinese activities in the information domain and resiliency for U.S. C4ISR capabilities.

How China Views the Space and Network Domains

China considers the space and network domains to be closely interlinked, with both being part of a broader concept they call the 'information domain'.[2] The information domain refers to the streams of information and data that underpin all modern systems relevant to a military conflict. It contains "systems of systems" built on and dependent upon network linkages between computers, space assets, sensors, and other information assets. This type of confrontation requires space superiority (制天权) and network superiority (制网络权), or the enabling of one's own operations in these domains while denying them to an adversary. In any future conflict, "seizing space superiority and network superiority will be key to obtaining comprehensive superiority on the battlefield."[3] Space superiority is particularly important, as it has "a decisive effect on network

[1] Although many Chinese sources may use the Western term "cyber" (赛博 / *sai bo*), most military writings use "network" (网络). While the definitions largely match, the PLA definition of "network" emphasizes the widespread end-users and nodes comprising networks, making it a useful term and construct for the information domain that comprises myriad platforms across multiple domains.

[2] The electromagnetic domain is also part of this broader information domain. Though my comments focus only on two legs of this information triad, it is impossible to understate the importance of electromagnetic means affect both.

[3] Shou Xiaosong, ed., *The Science of Military Strategy* (Zhanlue Xue / 战略学), Beijing, AMS Press, 2013, p. 96. The *Science of Military Strategy*, published by the Academy of Military Science, is a military teaching text and reference material for senior PLA officers, and offers authoritative views of PLA strategy. Another version, published in 2015

spaces and other military domains," and without it the dominance of any other domains is out of the question.[4]

China's emphasis on dominance in both domains traces back to the 1991 Gulf War, when it observed the role of C4ISR capabilities in the U.S. military's decisive victory. This interest grew when the role of satellites in U.S. C4ISR capabilities became even more apparent in the Kosovo War. Chinese military theorists described these conflicts as constituting a new 'informatized' mode of warfare, in contrast to the previous 'mechanized' mode. Before long PLA strategic thought shifted toward determining how best to prepare for fighting and winning informatized wars. In 2004, then paramount leader Hu Jintao issued the PLA its 'New Historic Missions' (新的历史使命), which in part called on PLA forces to defend China's interests in the new domains of distant oceans, outer space, and cyberspace. The 2013 revision of the influential *Science of Military Strategy* emphasized the centrality of conflict in the information domain.[5] By 2015, China's authoritative defense white paper on military strategy codified this prioritization by stating that "outer space and cyberspace have become new commanding heights in strategic competition among all parties."[6]

China's Aggressive Military Doctrine for Network Attacks against U.S. Space Assets

China's views of the space and network domains and the nature of informatized war inform an aggressive counterspace doctrine against U.S. C4ISR capabilities and for utilizing network attacks. In many of China's military writings, I would argue there are three key assumptions. First is that information systems depend on space-based assets and serve as the "brains" or "minds" for all U.S. forces in the Pacific theater. The second and corollary assumption is that if the PLA sufficiently threatens, degrades, or destroys such systems, the United States will stand down or its forces will face substantial delays entering the theater. The third assumption is that network attacks can be deployed effectively and with smaller risks of escalation. As an observation, what is also striking to me is that as China fields more satellites and projects power abroad, there is little to no acknowledgement that China may face these same vulnerabilities.

Many sources emphasize the importance of C4ISR capabilities, particularly those in the space domain, and how devastating their loss would be for a military force. Borrowing from British military historian and strategist J.F.C. Fuller, one text argues war has evolved from a "war of bodies," or one military organization versus another, into a "war of minds" (头脑战争), in which the objective is to attack command and control systems.[7] Other sources describe space-based communication links as the "backbone" of modern militaries and joint operations, and attacking space reconnaissance systems as "covering up the eyes and ears" of military forces. Targeted attacks against space-based assets can "paralyze command and control systems" and negate

by China's National Defense University, is also authoritative. This testimony draws from both, referring to them as the 2013 *SMS* and 2015 *SMS* respectively.

[4] Xiao Tianliang, ed., *The Science of Military Strategy* (Zhanlue Xue / 战略学), Beijing, NDU Press, 2015, p. 137

[5] Shou, ed., *The Science of Military Strategy*, 2013.

[6] The State Council Information Office of the People's Republic of China, "China's Military Strategy," May 2015.

[7] Jiang Lianju and Wang Liwen (eds.), *Textbook for the Study of Space Operations* (空间作战学教程), Beijing, Military Science Publishing House, 2013, p. 14

advantages of long-range precision strikes and carrier groups by cutting off information flows.[8] The bottom line is that (in the Chinese view) space and network capabilities can deliver a devastating blow that will negate or severely limit the U.S. military's ability to operate in theater.

The 2015 *SMS* describes network attack capabilities against space-based assets as providing both strategic and tactical-level deterrent value. "Strategic-level network deterrence" (战略级网络威慑) is defined as network attacks and demonstrations of capabilities against an enemy's political, military, and economic targets. C4ISR is the first example, followed by national transportation hubs and communication backbones. "Tactical-level network deterrence" (战术级网络威慑) emphasizes small-scale network attacks and network intrusions in order to "safeguard national security in peacetime."[9]

Network or cyberattacks on space assets are frequently mentioned as an ideal non-kinetic attack method in Chinese military writings on counterspace operations. PLA texts on space operations list network attacks as one of three primary types of "soft kill" or "non-kinetic" methods for attacking satellites,[10] and are well-versed in their advantages and disadvantages. Network attack methods are better for surprise and concealment compared to hard-kill methods such as kinetic kill vehicles (KKVs), and can paralyze an entire system instead of destroying one platform.[11] Additionally, KKVs produce a tremendous amount of space debris, as seen in China's ASAT test in 2007 and the recent Indian test.

Network (and electromagnetic) methods are "information weapons" (信息武器) that can capture, interfere with, block, and deceive adversary space-based information systems to the point of blockading, destroying, or paralyzing them.[12] According to one military textbook, the two primary types of network attack methods are: [13]

> (1) Breaking satellite signals to obtain their data link parameters and communications protocols, and using them to transmit viruses, logic bombs, and false information signals to cause malfunctions and paralysis of systems.
>
> (2) In advance of conflicts, placing viruses in enemy satellite information system computers, and when necessary activating the virus to destroy the system.

These weapons support "information blockades" (信息封锁), a type of space operation that envisions using all methods of information warfare to interfere with and destroy communication links between an adversary's space assets and ground stations and end-users. Other listed objectives are blinding surveillance equipment, disrupting space-based communications and operational links, and interfering with guidance and positioning signals.[14] The last objective deserves emphasis as the U.S. Navy mandated that probes of potential cyber tampering and cyber

[8] Chen Baoquan, Yang Guang, and Li Xuefeng, "Research on System Combat Effects and Develop Policy of Space Electronic Attack" (空间电子攻击的体系作战效用及发展对策), *Aerospace Electronic Warfare* (航天电子对抗), No. 28, Issue 1, 2012, pp. 11-13, 22-23.

[9] Xiao, *The Science of Military Strategy*, 2015, p. 147.

[10] The other two types are electromagnetic attacks and low-energy (such as laser and microwave) attacks.

[11] Jiang and Wang, *Textbook for the Study of Space Operations*, p. 48.

[12] Deng Jiekun, Shi Tongye, and Xie Jing, "ECM Capabilities of Space Information System" (空间信息对抗能力分析), *Aerospace Electronic Warfare* (航天电子对抗), No. 28, Issue 4, 2012, p. 4-6, 28.

[13] Jiang and Wang, *Textbook for the Study of Space Operations*, p. 121

[14] Ibid., pp. 134-135

intrusions be made standard parts of accident investigations following the 2017 collisions involving the USS *John S. McCain* and the USS *Fitzgerald*.[15]

One alarming aspect of China's military writings on space warfare strategy is the justification of targeting civilian satellites. According to *Study of Space Operations*, civilian assets are more numerous and may be more advanced than military systems, and carried 40% of U.S. communications in the Gulf War and 60% in the Kosovo War.[16] In a Taiwan scenario, a professor and graduate students with the former Second Artillery Engineering University clearly consider any "blue" satellites supporting "grey" Taiwanese "separatists" to be legitimate targets.[17] Recently, U.S. scholars and industry partners have raised the alarm that many new small satellites use unencrypted communications channels while operating in high-value orbital regimes, and are calling for industry self-regulation to encrypt such channels for some degree of protection from unauthorized users.[18] Any steps by the growing space industry to 'bake in' security measures should be encouraged as orbits become more crowded with increasingly capable commercial satellites.

Evidence of Chinese Network Attacks on Space Assets

As early as 2007, PLA authors spoke candidly about how hackers can use satellite signals to take over its command control network, and then give commands over a basic internet connection.[19] Notably, in that year and in 2008 at least two U.S. government satellites (Landsat 7 and Terra (EOS AM-1) satellites) operated by NASA and USGS.[20] Since then, China has been suspected of multiple hacks against entities responsible for managing space assets, though no hack of a satellite has been reported in the open source. Reported events include:

> 2010 to 2011: The NASA Jet Propulsion Laboratory suffered an attack involving IP addresses based in China, and confirmed that intruders had full access to key systems and sensitive user accounts. "In other words, the attackers had full functional control over these networks."[21]

[15] Sam LaGrone, "Cyber Probes to be Part of All Future Navy Mishap Investigations after USS John S. McCain Collision," *USNI News*, September 14, 2017. https://news.usni.org/2017/09/14/cyber-probes-part-future-navy-mishap-investigations-uss-john-s-mccain-collision

[16] Jiang and Wang, *Textbook for the Study of Space Operations*, p. 73.

[17] Yu Ming, Bi Yiming, and Deng Penghua, "Research on Capacity Demand of Kinetic Energy Anti-Satellite Maneuver" (地基动能反卫星作战能力需求研究), *Ordnance Industry Automation* (兵工自动化), No. 9, 2012, pp. 1-3.

[18] A. Kurzrok, M. Diaz Ramos, and F. S. Mechentel, "Evaluating the Risk Posed by Propulsive Small-satellites with Unencrypted Communications Channels to High-Value Orbital Regimes," 32nd Annual AIAA/USU Conference on Small Satellites.

[19] Xiao Wenguang and Li Yuanlei, "Computer Networks in Future Wars" (计算机网络于未来战争), *Jiangsu Aviation* (江苏航空), No. 1, 2007, p. 31.

[20] U.S.-China Economic and Security Review Commission, *2011 Report to Congress of the U.S.-China Economic and Security Review Commission: One Hundred Twelfth Congress, First Session*, Washington, DC, U.S. G.P.O., p. 216. https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

[21] "NASA Cybersecurity: An Examination of the Agency's Information Security," Statement of Paul K. Martin, Inspector General, National Aeronautics and Space Administration, testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology, February 29, 2012. https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

> 2014: NOAA reported that its networks were hacked, “forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses.” According to Rep. Frank Wolf, NOAA confirmed to him that China was responsible for the attack.[22]
>
> 2018: Security researchers at Symantec Corp reported on a hacking campaign from China against “satellite operators, defense contractors and telecommunications companies in the United States and southeast Asia.” [23]

Another worrisome threat in the network and space domains is China’s development of generative adversarial networks (GANs), an emerging artificial intelligence (AI) method for tricking computer programs into seeing objects in imagery that are not there. According to one expert, China is already using GANs “to manipulate scenes and pixels to create things for nefarious reasons.”[24] If successful, GANs could poison data feeds of imagery collection for analysts and raise doubts in force planning.

The Strategic Support Force: Force for Informatized Warfare

In the last five years, China has dramatically reoriented its armed forces in response to this reality. The establishment of the Strategic Support Force reflects both a culmination of military thinking on these (and other) domains, as well as an acknowledgement of China’s growing interest in them. Applying a holistic approach to information warfare, the SSF bridges gaps within and between domains (especially network and space), and provides China’s leadership with a centralized entity for deploying a whole suite of non-kinetic options for information operations that can scale across domains and across the world.

The SSF utilizes an organizational structure that is domain-centric rather than function or discipline-centric, with the bulk of its forces divided into its Network Systems Department (网络系统部) and Space Systems Department (航天系统部).[25] In a contrast with the previous GSD model, wherein the former GSD Third Department (3PLA) generally handled espionage and the former GSD Fourth Department (4PLA) handled offensive computer network operations, these functions are integrated under the SSF Network Systems Department. Meanwhile, the Space Systems Department resolves the bureaucratic competition between the PLA Air Force, the former General Armament Department, and other entities for the space mission by taking control of many space-based and space-related assets.

In theory, this domain-centric model facilitates the broader strategy of Mao’s dictum to “integrate peacetime and wartime” (平战结合), meaning that peacetime organization and activities should

[22] Mary Pat Flaherty, Jason Samenow, and Lisa Rein, “Chinese Hack U.S. Weather Systems, Satellite Network,” *Washington Post*, November 12, 2014. https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?noredirect=on&utm_term=.aa9ccd99601b

[23] Joseph Menn, “China-based Campaign Breached Satellite, Defense Companies: Symantec,” Reuters, June 19, 2018. https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0

[24]

[25] Elsa Kania and John Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” *The Cyber Defense Review*, Vol. 3, No. 1, Spring 2018, pp. 109-110.

reflect as much as possible their wartime counterparts.[26] Prior to the SSF's establishment, one author described "space information network conflict" (空间信息网络对抗) as being about "integrating space technology and network countermeasure technologies as a strategy to seize network superiority as a goal." The required methods span (and indeed blur) the lines between peace and wartime measures, such as surveillance of enemy networks; the use of wireless intrusion tactics to identify weak links in enemy information network systems and their transmissions; the use of integrated network and electronic warfare (INEW / 网电一体战), including malware and electromagnetic signals, to disrupt enemy information systems; and preparations for soft (such as network-based) and hard kill methods against space-based assets. [27]

The SSF's structure is well-suited at least on paper for all of the above missions and operations. However, the success or failure of the SSF to achieve the goals set out for it will ultimately depend upon the PLA's ability to effectively command and coordinate these forces to achieve desired effects. The SSF is still relatively new, and likely experiencing growing pains of any new bureaucracy. Some challenges or disadvantages to this model could include:

> (1) The creation of the SSF clearly reflects Chinese strategic thinking, but it is not yet proven that the new structure is better than the previous one. Any reorganization produces winners (SSF, PLA Rocket Force) and losers (PLA Army, GSD). In this case, is the SSF a full-fledged service/branch, with its own institutional agenda and bargaining power, or is it a loose agglomeration of assets and capabilities culled from other services, branches, and organizations? The answer to this question will go a long way in determining how effectively the PLA will develop and employ its capabilities in the new domains.
>
> (2) If everything is strategic, nothing is strategic. Efficiency and decisiveness can be impeded if central leaderships determines that all or most of the PLA's space, network, and electromagnetic operations require centralized command. It is not clear yet clear who would exercise command authority over SSF operations in wartime.
>
> (3) As the PLA expands its operations abroad, it will feel the growing pains of becoming a global military force, and expanded deployments could exacerbate any existing challenges. Currently it is unclear what role the SSF will play in overseas operations and how it will be deployed to support China's interests abroad.

Recommendations

China is clearly exerting tremendous efforts to compete and win in the space and network domains. In response, I offer three policy suggestions for the United States Congress:

1. Prioritize constant monitoring and vigilance in the information domain.

Congress should ask the Department of Defense and entities like the USCC to prioritize studies of China's information warfare strategy and programs at both the classified and unclassified levels.

[26] He Quansheng (贺全胜), "On the Development and Implications of Mao Zedong's People's Militia Thought" (论毛泽东民兵思想的发展与内涵), CCCPC Party Literature Research Office, 2016, https://www.wxyjs.org.cn/ddwxzzs/wzjx/201605/201610/t20161015_218637.htm.

[27] Huang, "Study on the Space Network Countermeasures."

The establishment of the SSF is China's most forceful move to date in a new domain that will play a decisive role in any future conflict. The lack of discussions on China's own vulnerabilities in the space domain also warrants monitoring, as the silence may indicate a lack of awareness, a higher acceptance of risk, or censorship. Technical experts are also needed for these efforts, as both domains are already technologically demanding and now face new threats from emerging technologies like artificial intelligence. The U.S. military, political leaders, and diplomats need high-fidelity assessments of China's intent and progress in the information domain in order to inform strategy, any potential military exchanges, and strategic signaling in a potential crisis or conflict.

2. Support resiliency of C4ISR and all information support systems.

Congress should support any DOD or other agency efforts that build resiliency into information support systems. Measures could support existing C4ISR capabilities, such as enhancing capabilities for rapid launch of replacement satellites, or could improve U.S. forces' ability to operate under degraded information conditions with alternatives to space-based assets. In monitoring and evaluating the readiness of U.S. forces, the ability to operate under degraded information conditions should be the gold standard of readiness.

3. Support measures for supply chain security of U.S. information systems.

Congress should prioritize supply chain integrity in government and defense procurement policies. The globalization of technology industries and supply chains has brought tremendous innovation and economic growth, but key sectors like semiconductors require a calibrated policy that accounts for security risks and invests in the on-shoring of core manufacturing capabilities. Today, China poses a threat to the DOD's microelectronics supply chain, with over 50 percent of the Pentagon's purchased microelectronics being sourced from the country.[28] At the same time, China is investing vast resources into research, development, and manufacturing for advanced sectors like advanced computing and semiconductors. The entire information domain rides on such systems, and demands greater supply chain integrity measures. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) is a good start at protecting key capabilities from being acquired and outsourced, but more is needed. A 2018 report by the DOD's Office of Industrial Policy provides an excellent assessment of current risks and options for remedying them.[29]

[28] John Harper, "China Threatens Microelectronics Supply Chain, DoD Official Says," *National Defense Magazine*, December 19, 2017. http://www.nationaldefensemagazine.org/articles/2017/12/19/china-threatens-microelectronics-supply-chain-dod-official-says

[29] Department of Defense, Office of Industrial Policy, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," September 2018. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF