INFORMATION DOMINANCE:
THE IMPORTANCE OF INFORMATION AND OUTER SPACE IN CHINESE THINKING

Chairman Yoho, Ranking Member Sherman, and Members of the House Foreign Affairs Committee. Thank you for the opportunity to testify to you this afternoon.

My name is Dean Cheng and I am Senior Research Fellow in the Asian Studies Center of the Davis Institute for National Security and Foreign Policy at The Heritage Foundation. My comments today are purely my own and should not be construed as representing any official position of The Heritage Foundation.

My comments today focus on the evolving views of the People's Republic of China (PRC) regarding the role and importance of information. Note that this is not only a matter of the role of information in open warfare, but also its place in the strategic competition in which the United States and the PRC already find themselves.

Growing Role of Information in War and Peace

From the Chinese perspective, these changes in the role of information are based on the fundamental shift in global socioeconomic conditions. The 20th Century was characterized by the Industrial Age. The very fundamentals of power were rooted in industrial capacity. Nations were measured and compared by their industrial capacity. Wars were won, not only by masses of tanks, ships, and aircraft, but the possession of the industrial base necessary to produce those weapons.

By contrast, in the Chinese view, the 21st Century is marked by the Information Age. Where national power was once a function of gigawatts of generating capacity and tons of iron smelted, it is now more a function of the ability to gather, analyze, and exploit information. The rise of telecommunications, the global Internet, and massive advances in computing power now provide unprecedented global access to information—and therefore the ability to inform but also to influence. This increasing centrality of information is termed "informationization" (*xinxihua*; 信息化).

Just as informationization has affected global economy and society, it has also influenced the nature of war. War, from the PRC's perspective, is a function of not just military forces and politics, but also reflects larger social, economic, and technological trends. The rise of the Information Age, marked by the widespread integration of information and information technology into all aspects of modern society and economics, also affects the nature of conflict, leading to "informationized warfare" (*xinxihua zhanzheng*; 信息化战争).

What is essential to recognize is that, for the Chinese, both information extraction and information exploitation, which are central to establishing information dominance:

- Are essential to modern warfare;
- Must occur in peacetime, in order to be useful in wartime; and
- Go far beyond purely military-related information, and includes economic and political information.

The PLA and Information

A key player in Chinese efforts to compete in an informationized world is the People's Liberation Army (PLA). The PLA is not a national military, but is first and foremost a ***Party army***. Indeed, the PLA is the armed wing of the Chinese Communist Party (CCP). Therefore, it does the Party's bidding, including keeping the Party in power.

Its actions are therefore not those of a "rogue" military. As important, they are undertaken in support of broader national goals and polices, as set forth by the CCP, in support of expanding the power of both the Chinese state and the Party itself. Thus, it is entirely consistent with the roles and missions of the PLA for it to be tasked with obtaining industrial and economic information, as well as military codes and war plans.

Furthermore, this is not "your father's PLA." This is no longer a PLA that is focused primarily on quantity. It is, instead, a learning organization that has paid close attention to other peoples' wars, in part because it has not fought one itself since 1979. As a learning organization, it has been adapting to the changing circumstances of modern warfare, adopting fundamentally new approaches to conflict.

Consequently, the PLA has been increasingly focusing on high technology and high-tech wars, dating back to at least the first Gulf War. From that conflict, and the Balkan wars of the 1990s, the PLA concluded that future wars would be joint, not only involving the ground forces, navy, and air force, but involving operations across the domains of land, sea, air, outer space, and information space (which includes cyberspace).

As the PLA observed in subsequent conflicts including those in Afghanistan and Iraq, however, their views of future warfare further evolved. In order to operate effectively across the various domains, the PLA would need to establish common situational awareness. Jointness was no longer a matter of getting air, land, and sea forces in the same operational volume, but it involved allowing ground forces to get targeting information from air units, and naval forces to support air and land forces. For the PLA, this meant that not all high technology was created equal—the most important technologies were those associated with information, including telecommunications, computing, and space.

This shift reflected the informationization of warfare, where information was applied to all aspects of warfare. This includes not just weapons, but logistics, personnel selection and management, and decision making.

Informationization of Conflict

According to the PLA's volume on terminology, informationized warfare is warfare where there is widespread use of informationized weapons and equipment and networked information systems, employing suitable tactics, in joint operations in the land, sea, air, outer space, and electromagnetic domains, as well as the cognitive arena. Informationized warfare in turn involves informationized militaries, which will operate through networked combat systems, command-and-control systems, and logistics and support systems, as part of the systems-of-systems construct.

The focus of informationized warfare is establishing "information dominance" (*zhi xinxi quan*; 制信息权). This is the ability to establish control of information and information flow at a particular

time and within a particular space.[1] It entails the ability to collect more information, manage and analyze it faster, and employ it more precisely than the adversary.[2] In doing so, in the Chinese view, the side that enjoys information dominance can seize and retain the initiative, and force the adversary into a reactive mode. This exploits a key difference between mechanized warfare of the Industrial Age, and informationized warfare of the Information Age. "Mechanized warfare focuses on physically and materially destroying an opponent, whereas informationized warfare focuses on inducing the collapse of the opponent's psychology and will."[3]

Establishing information dominance entails efforts that span the strategic to the tactical level. It is not simply a wartime requirement, but involves intelligence gathering throughout peacetime. Because of the rapid, decisive nature of "local wars under informationized conditions," it is not possible to wait until the formal commencement of hostilities to begin preparations. At a minimum, identifying opposition capabilities and weaknesses must be undertaken in peacetime.

Nor can this be solely a military function. As the world has informationized, the Chinese economy has had to informationize; similarly, as warfare has informationized, the Chinese military has had to evolve to prepare to fight such conflicts. Although the PLA plays a major role, though, such preparations involve all the various elements of the Chinese government and broader society and economy. Because of the interconnected nature of modern information networks, and their extensive permeation, information dominance involves gaining access not only to the adversary's military networks but to decision makers and the broader population, while defending against their efforts to do the same. As important, since information itself can be used as a weapon (beyond the incorporation of viruses and malware) by influencing its consumers, it is essential that information itself be monitored and information flow be tightly controlled, from a defensive perspective.

---

[1]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume) (Beijing, PRC: Military Science Publishing House, 2011), p. 79.

[2]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, 2nd Edition, *Military Strategy* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 68.

[3]Fan Gaoming, "Public Opinion Warfare, Psychological Warfare, and Legal Warfare, the Three Major Combat Methods to Rapidly Achieving Victory in War," *Global Times* (March 8, 2005), http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/mil/2005-03/08/content_2666475.htm (accessed April 21, 2017).

Similarly, establishing information dominance involves a multi-pronged effort, addressing all aspects of information. Not only is it necessary to target an adversary's data, but also the systems involved in data collection and management, as well as the users and analysts of data. Similarly, it requires defending all three aspects of one's own information architecture, i.e., data, systems, and users.

The human element is especially important in informationized warfare. Chinese analysts note that the advent of more advanced weapons technologies did not necessarily lead to a change in the basic nature of war. Instead, the core of informationized warfare is the expanded range of abilities to influence and control an opponent's judgment and will to fight.[4] The ability to influence people, in terms of their politics, their thinking, their morale and spirit, and their psychology can be as decisive and effective as the ability to interfere with databases or computer networks. The ability to influence an adversary through the proper application of suitable information is embodied in the Chinese concept of political warfare.

Thus, at the strategic level, informationized conflict means using information to influence perceptions of the PRC and the United States. Is China engaging in aggression in the South China Sea, or is it defending its long-standing historic claims? The answer is based upon one's perceptions of China and China's actions, and influencing those perceptions is the focus of Chinese political warfare efforts.

In particular, political warfare for the PRC includes the "three warfares." These are the hardest forms of soft power, used to affect the thinking and psychology of the domestic Chinese audience, the adversary's leadership and population, and the views of third parties. Each of the three "warfares" employs information in a different manner to achieve these goals, but reinforces the other two.

Psychological warfare exploits information by drawing upon the political, economic, and cultural, as well as military elements of power. Information of each type can serve as a powerful weapon,

[4]Chang Long, "Tightly Grasping the Trends of the New Military Transformation—Reflections and Outlook from the Gulf War to the Iraq War," *PLA Daily*, October 28, 2003, http://www.xslx.com/htm/gjzl/jsgc/2003-10-38-15176.htm (accessed April 21, 2017).

influencing values, concepts, emotions, and context.[5] Legal warfare can build psychological support and sympathy among bystanders, and erode an opponent's will by constraining their preferred courses of action for fear of legal repercussions. Public opinion warfare can directly build support, persuading domestic and foreign audiences of the justice of one's own cause and the success of one's own efforts, while undermining an adversary's attempts to do the same. In particular, the growth and expanded reach of media of various sorts makes public opinion warfare especially important, as it can have global effects. Broad domestic and international support, in turn, will generate psychological benefits for oneself and adversely affect the enemy.

Chinese analysts see "public opinion warfare" (*yulun zhan*; 舆论战) as a special part of informationized warfare. Because of the wide permeation of information technology, public opinion warfare has global reach, extends to every part of society, and has an especially wide impact. The goal of public opinion warfare is to shape public and decision-maker perceptions and opinion, so as to shift the perception of overall balance of strength between oneself and one's opponent.[6] To this end, it is especially important that communications efforts associated with public opinion warfare be mutually reconciled and coordinated, so that specific messages are clearly transmitted, in support of specific goals. While the news media plays an important role in the Chinese conception of public opinion warfare, it is only a subset of the larger set of means available for influencing public opinion.[7]

Public opinion warfare supports psychological warfare. This pressures an opponent by employing information to affect their thinking, to create damaging or deleterious habits and ways of thinking, to reduce their will to resist.[8] At the same time, it seeks to limit the effect of enemy psychological warfare operations on one's own troops, population, and leadership, building morale, encouraging greater resistance and effort, and strengthening will.

---

[5]Tan Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology* No. 5, 2009, p. 73.

[6]Academy of Military Sciences Operations Theory and Regulations Research Department and Informationalized Operations Theory Research Office, *Informationalized Operations Theory Study Guide* (Beijing, PRC: AMS Press, November, 2005), p. 405, and Liu Gaoping, *Study Volume on Public Opinion Warfare* (Beijing, PRC: NDU Press, 2005), pp. 16–17.

[7]Liu, *Study Volume on Public Opinion Warfare*, p. 5.

[8]Tan Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," p. 76.

Psychological operations are seen as an essential part of future conflicts, affecting and influencing, at a basic level, the very perceptions that inform decision making, from the context to the biases. Successful psychological operations in informationized warfare will therefore have repercussions at strategic, operational, and tactical levels of operations, influencing both military and civilian leaders as well as the masses, and thereby affecting the course of the conflict.

Legal warfare questions the basic legitimacy of adversary actions. It involves "controlling the enemy through the law, or using the law to constrain the enemy (*yifa zhidi huo yong fa zhi di*; 以法制敌 或 用法制敌)."[9]

Legal warfare depicts "one's own side is obeying the law, criticizing the other side for violating the law (*weifa*; 违法), and making arguments for one's own side in cases where there are also violations of the law."[10] The ultimate goal is to secure the initiative in time of conflict, by gaining the legal high ground, portraying oneself as the side more firmly grounded in legal standing, and implicitly as being more virtuous and just.

Information warfare is the operational application and realization of informationized warfare. It is the conduct of warfare through the application of information and information technology in modern warfare. The priorities are on "network warfare," which is not just cyber, but all types of networks, and electronic warfare, which goes beyond jamming radars and radios. Indeed, the Chinese see the two as fundamentally linked, in the form of "integrated network and electronic warfare."

This is supplemented by psychological warfare. Here, it is an effort to influence the adversary's thoughts, emotions, knowledge, perspectives, and attitudes.[11] Through the application of various forms of information, psychological warfare strives to alter the adversary's interpretations of

[9]Zong Wenshen, *Legal Warfare: Discussion of 100 Examples and Solutions* (Beijing, PRC: PLA Publishing House, 2004), p. 5.

[10]Han Yanrong, "Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong," *Legal Daily* (PRC), February 12, 2006.

[11]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), (Beijing, PRC: Military Science Publishing House, 2011), p. 456, and Ye Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), pp. 25–26.

information, including their context and frame of reference, as well as to undermine their will.[12] The purpose of psychological warfare at the operational level is to buckle the adversary's will and martial spirit, induce confusion in their command and decision-making processes, especially for military functions, and shake their confidence in their capabilities and ability to win, so as to reduce their combat effectiveness.[13]

In addition to electronic warfare, network warfare, and psychological warfare, there has been a growing discussion in the Chinese literature of "command and control warfare" and "intelligence warfare." The idea is that the key electronics, networks, and decision makers are those that are part of the intelligence network and the command-and-control structure.

At the tactical level, the Chinese conduct information operations. This includes the combination of hard-kill and soft-kill techniques. Just as information warfare sees "integrated network-electronic warfare," Chinese views of information operations include "integrated firepower-information attacks." The physical infrastructure is seen as important, alongside the computers and data. Some targets may be jammed, others hacked or infected with viruses, but in some cases, it might involve physical destruction of a server farm or a command-and-control center. This might involve special operations forces or it might involve precision-guided munitions.

This places China's increasing role in the construction of the physical part of the Internet in a different light. The ability of China to build information systems in Africa, South America, Central Asia, and Europe means that, in the future, China will have insight, and possibly access, to much of the physical infrastructure over which information passes. At the same time, including Chinese laptops and smart phones in critical communications networks means that the point of connecting to the network is also more and more often "made in China."

China's Growing Space Capabilities

An important part of the physical infrastructure for information-space is outer space. Space is a central means of obtaining information, including not only support to military operations, but for

[12]Wu Renhe, *Theory of Informationized Conflict* (Beijing, PRC: Military Science Publishing House, 2004), p. 192.

[13]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, 2nd Edition, *Military Psychology* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 67.

agricultural, industrial, and commercial purposes. Indeed, it has been suggested that 95 percent of space technology is dual-use in nature.[14] Space plays an essential role in the Information Age for military and civilian functions.

Along these lines, PLA analyses suggest that it views space in a very holistic fashion. Chinese writings note that the overall space system encompasses not only satellites in orbit, but also terrestrial launch, mission control, and tracking, telemetry and control (TT&C) facilities, as well as the data links that tie the space and Earth-bound portions together. Consequently, efforts aimed at establishing space dominance must incorporate offensive and defensive measures covering this full range of targets (orbiting systems, ground-based systems, data). "Space dominance" (*zhitian quan*; 制天权) is defined as "the ability by one side in a conflict to control [or dominate] a certain portion of outer space at a given time." The goal is to secure the advantage in space, ensuring that one's own side has freedom of action in space, while constraining the other side's comparable freedom of action in space.[15]

The Chinese interest in space dominance has been noted in the assessments of American intelligence agencies. General Vincent Stewart of the Defense Intelligence Agency testified in 2015 that several nations, including China, are developing counter-space capabilities.

> The threat to U.S. space systems and services will increase as potential adversaries pursue disruptive and destructive counterspace capabilities.… Chinese and Russian military leaders understand the unique information advantages afforded by space systems and are developing capabilities to deny U.S. use of space in the event of a conflict. Chinese military writings specifically highlight the need to interfere with, damage, and destroy reconnaissance, navigation, and communication satellites.[16]

The importance of being able to guarantee Chinese interests in the space domain was underscored in the "new historic missions" that Hu Jintao charged the PLA. In his 2004 speech,

---

[14]Roger Cliff, *The Military Potential of China's Commercial Technology* (Santa Monica, CA: RAND Corporation, 2001), p. 27, https://www.rand.org/content/dam/rand/pubs/monograph_reports/2001/MR1292.pdf (accessed April 21, 2017).

[15]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *Military Strategy*, *Chinese Military Encyclopedia* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 211.

[16]Ltg Vincent R. Stewart, "Worldwide Threat Assessment 2015," testimony before the Armed Services Committee, U.S. House of Representatives, February 3, 2015, http://www.dia.mil/News/SpeechesandTestimonies/tabid/7031/Article/13225/worldwide-threat-assessment.aspx (accessed April 21, 2017).

Hu stated that one of the new missions for the PLA is to provide strong strategic support for maintaining national interests. In light of national development and broader global trends, Hu observed that China's national interests and security had gone beyond the traditional land, sea, and air and shifted towards the oceans, space, and the electromagnetic domain. "Maritime security, space security, electromagnetic spectrum security," he noted, "are already vital regions for national security," where a small number of major powers are seeking to secure the advantage. Hu elevates space security, along with maritime security and electromagnetic security, to the equivalent of the security of land, sea, and air territories.[17]

Subsequent Chinese writings have reflected this growing importance of space. The 2013 volume *The Science of Military Strategy*, published by the Chinese Academy of Military Science, for example, includes a chapter devoted to discussing military conflict in the space and cyber (as well as nuclear) domains. In this extensive revision of the 2001 version, it is noted that the importance of space has grown significantly for both military and broader national purposes.[18] The competition to dominate space is steadily intensifying, involving not only major powers, but even mid-size powers. Successful military strategy therefore demands the ability to successfully conduct space information support, space deterrent activities, and both offensive and defensive operations in space. Moreover, space deterrence, to be credible, must include offensive capabilities. Similarly, fielding offensive, as well as defensive, capabilities in space strengthens space deterrence.

Similarly, the new 2007 edition of the *PLA Encyclopedia* also discusses space dominance. It notes that space dominance is "a vital factor in securing air dominance, maritime dominance, and electromagnetic dominance, and will directly affect the course and outcome of wars."[19]

Military space operations, including the need to secure space dominance, are also discussed in other Chinese materials. In a volume jointly authored by the Academy of Military Science Operations Theory and Regulations Research Department and the Informationized Operations

---

[17]Hu Jintao, "Understanding Our Military's New Historic Missions in the New Phase of the New Century," December 24, 2004, http://gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml (accessed April 21, 2017).

[18]AMS Military Strategy Research Department, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), pp. 178–188.

[19]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *Military Strategy*, *Chinese Military Encyclopedia* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 211.

Theory Research Office, it is noted that "in future informationized wars, securing the space advantage, obtaining space dominance, will be the prerequisite for securing the initiative in the war."[20] Similarly, PLA teaching materials on joint campaigns observe that "without space dominance, it is difficult to assure the smooth operation of space information systems, which will make it hard to assure the smooth operation of military information systems, which in the end will mean that it is difficult to secure battlefield information dominance."[21]

Chinese Space Weapons Developments. China's interest in military space activities are not limited to hypothetical analyses. China has conducted a number of weapons tests and other activities that suggest an ongoing array of weapons development efforts. These include a number of different anti-satellite vehicles, as well as possible directed energy weapons (e.g., lasers). Chinese cyber capabilities may also have anti-satellite functions (among others); similarly, Chinese conventional modernization may allow them to hold some of the terrestrial elements of the American (and allied) space infrastructure at risk.

Ground-Launched Anti-Satellite Systems. In January 2007, China tested a direct-ascent kinetic kill vehicle against a defunct FY-1C weather satellite, resulting in one of the worst debris-generating events in space history. This test, according to Paula DeSutter, then Assistant Secretary of State for Verification, Compliance, and Implementation, was not the first test, however, but followed two earlier non-destructive tests of the same system.[22] This ongoing development program does not appear to have ended, although there have not been any comparable tests since 2007.

Since then, however, China ***has*** conducted three tests of a ballistic missile defense system that might also have anti-satellite applications. In 2010, the Chinese "conducted a test on ground-based midcourse missile interception technology within its territory."[23] As American defense

---

[20]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide—400 Questions on Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2005), p. 278.

[21]Li Yousheng, *Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 69.

[22]Lon Rains and Colin Clark, "Profile: Keeping a Watch on U.S. Interests," *Space News*, March 1, 2007, http://spacenews.com/profile-keeping-watch-us-interests/ (accessed April 21, 2017).

[23]"China Reaffirms Its Missile Test Defensive," *Xinhua*, January 12, 2010, http://news.xinhuanet.com/english/2010-01/12/content_12797459.htm (accessed April 21, 2017).

officials noted, "We detected two geographically separated missile launch events with an exo-atmospheric collision also being observed by space-based sensors."[24] The Chinese conducted another missile defense test in January 2013, and used almost the exact same language to describe it, i.e., a midcourse missile interception. In July 2014, the Chinese conducted another test, which it has termed a missile defense test, but which the United States characterized as a non-destructive anti-satellite test.[25] It should be noted that these tests resemble the American interception of the satellite US193 with an AEGIS missile.

While these earlier tests were engaging targets in low-earth orbit (160–2,000 kilometers altitude), in 2013, China has also tested a ground-launched anti-satellite system that would appear to be able to threaten satellites in geosynchronous orbit (36,000 kilometers altitude).[26] This constitutes a substantial expansion of the potential threat posed by Chinese anti-satellite capabilities. As important, it would hold at risk a range of key satellites, including communications and missile early warning systems.

Co-Orbital Anti-Satellite Systems. The ability of satellites to maneuver together has both peaceful and military potential. Docking maneuvers are integral to such actions as resupply of the International Space Station and were fundamental to the American Moon landings. At the same time, however, any satellite, if it has sufficient fuel and can be finely controlled while guided by a sufficiently discerning tracking system, can serve as a co-orbital anti-satellite system; in effect, it would be a space kamikaze. Recent Chinese developments in small satellites and space robots, as well as manned space missions, have demonstrated an ability to maneuver satellites together.

In 2010, two Chinese small satellites, SJ-06F and SJ-12, engaged in a series of maneuvers that suggest a controlled conjunction, in which the two satellites "bumped."[27] The ability to

---

[24]"China: Missile Defense System Test Successful," *USAToday*, January 11, 2010, http://usatoday30.usatoday.com/news/world/2010-01-11-china-missile-defense_N.htm (accessed April 21, 2017).

[25]Mike Gruss, "U.S. State Department: China Tested Anti-Satellite Weapon," *Space News*, July 28, 2014, http://spacenews.com/41413us-state-department-china-tested-anti-satellite-weapon/ (accessed April 21, 2017).

[26]Brian Weeden, "Through a Glass, Darkly," Secure World Foundation, March 17, 2014, http://swfound.org/media/167224/Through_a_Glass_Darkly_March2014.pdf (accessed April 21, 2017).

[27]Brian Weeden, "Dancing in the Dark: The Orbital Rendezvous of SJ-06F and SJ-12," *The Space Review*, August 30, 2010, http://www.thespacereview.com/article/1689/1 (accessed April 21, 2017).

undertake controlled approaches reflects a nascent ability to steer a satellite, and to bring it into contact with another space system. Similarly, China's controlled docking maneuvers by the Shenzhou-VIII, Shenzhou-IX, and Shenzhou-X space capsules with the Tiangong space lab demonstrate China's ability to closely monitor spacecraft operations, including approach and contact. That Shenzhou-VIII was remotely docked via ground control also reflects Chinese ability to bring spacecraft into carefully controlled contact with each other.

In August 2013, China again demonstrated an ability to maneuver satellites in close proximity, as several Chinese satellites apparently maneuvered in a manner that again suggests that they may have physically contacted each other. One of the satellites may have been equipped with a robotic arm, adding an additional capability for servicing satellites—or damaging them while in orbit.[28]

Directed Energy Weapons. Chinese kinetic kill vehicles (KKV) tests have garnered significant commentary and discussion; less is known about Beijing's development of directed energy weapons (DEW). In 2006, China apparently fired lasers at American satellites passing overhead. Contemporary reporting indicated that this was one of a series of events involving Chinese lasers and American military or intelligence satellites.[29] While the United States expressed concern over what was then described as an anti-satellite system, subsequent reporting suggested that it was not clear whether these were, in fact, weapons, or laser ranging devices.[30] Other reports suggest an ongoing research effort into developing lasers for a variety of defense purposes, including anti-satellite functions.[31]

Cyber Capabilities. As noted earlier, the Chinese interest in counter-space is not limited to developing systems to attack orbiting satellites, but also extends to the ability to degrade or

---

[28]Kevin Pollpeter, "China's Space Robotic Arms Programs," Study of Innovation and Technology in China Project, October 2013, http://igcc.ucsd.edu/assets/001/505021.pdf (accessed April 21, 2017).

[29]Vago Muradian, "China Attempted to Blind U.S. Satellites with Laser," *Defense News*, September 25, 2006.

[30]"NRO Confirms Chinese Laser Test Illuminated US Spacecraft," *Space News*, October 3, 2006, http://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/ (accessed April 21, 2017), and "China Jamming Test Sparks US Concern," *USAToday*, October 5, 2006, http://usatoday30.usatoday.com/tech/news/2006-10-05-satellite-laser_x.htm (accessed April 21, 2017).

[31]Wendell Minnick, "China Pursues Systems to Keep US Forces at Bay," *Defense News*, September 17, 2013, http://archive.defensenews.com/article/20130917/DEFREG03/309160021/China-Pursues-Systems-Keep-US-Forces-Bay (accessed April 21, 2017).

damage datalinks that connect satellites to ground stations. Space dominance can be achieved if a key satellite is shut down, its mission payload is pointed in the wrong direction, or it is unable to communicate at critical moments, as if it had been destroyed by an anti-satellite system. Indeed, this may be a preferable outcome, since attribution may be difficult and such approaches are unlikely to generate space debris (and attendant political and diplomatic criticism). Consequently, Chinese cyber capabilities should be considered an integral part of China's "counterspace capabilities."

Several cyber incidents involving space systems have been attributed to the PRC, suggesting that they are actively exploring vulnerability in space information systems. Hacking incidents in 2007 and 2008 against the LANDSAT-7 and Terra AM-1 EOS (Earth Observation System) satellites reportedly allowed cyber-intruders to gain control over all functions of these satellites for several minutes.[32] The attacks have been attributed to the PRC. Other reports suggest that China is responsible for hacking into the National Oceanic and Atmospheric Administration's weather satellite system.[33]

These cyber activities are a reminder that the Chinese see cyber operations as a part of information operations, and that space networks are part of the broader information networks that the Chinese seek to disrupt. The focus is on ***information***, not just cyber or space.

The integrated manner in which China thinks of information operations and space activities is reflected in Chinese military developments of the past several years, which are themselves the culmination of nearly a quarter century of thought regarding the shape and requirements of future warfare. The recently announced Chinese military reforms, including the creation of the PLA Strategic Support Force (PLASSF), highlights this. The PLASSF includes China's space, cyber, and network warfare forces. It is fair to argue that it is better described as China's "information warfare" force.

---

[32]Tony Capaccio and Jeff Bliss, "Chinese Military Suspected in Hacker Attacks on U.S. Satellites," Bloomberg News, October 27, 2011, http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (accessed April 21, 2017).

[33]Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack Weather Systems, Satellite Network," *The Washington Post*, November 12, 2014, http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html (accessed April 21, 2017).