The Heritage Foundation

CONGRESSIONAL TESTIMONY

Getting to Where the PLA Needs to Be

Testimony before
U.S.–China Economic and Security Review Commission

June 20, 2019

Dean Cheng
Senior Research Fellow, Asian Studies Center
The Heritage Foundation

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

Introduction

Since the early 1990s, the People's Liberation Army (PLA) of the People's Republic of China (PRC) has been steadily evolving its approach to warfare. Not having fought a war since 1979, the Chinese military is forced to rely on other peoples' experiences, in other peoples' wars, to derive lessons about what future wars will be like. This includes drawing upon not only American military actions, but also Russian, as well as broader changes in the global social-economic-technological environment. The result has been an increasing emphasis on the role of information, and the belief that achieving "information dominance" will be essential in fighting and winning future wars.

Evolving View of Future Wars

In the wake of the first Gulf War (Operation Desert Shield/Desert Storm), the Chinese concluded that there was a need to prepare for what they termed "local wars under modern, high-technology conditions (*gao jishu tiaojian xia jubu zhanzheng*; 高技术条件下局部战争)." The characteristics of such wars included:

- The quality, as well as the quantity, of weapons matters. The side with more technologically sophisticated weapons would be able to determine the parameters of the conflict, and effectively control its scale and extent.

- The battlefields associated with such conflicts are three-dimensional, and extend farther and deeper into the strategic rear areas of the conflicting sides.
- The conflict is marked by high operational tempos conducted around the clock, under all-weather conditions.
- The fundamental approach to warfare is different. Such wars would place much greater emphasis on joint operations, while also incorporating more aerial combat, long-distance strike, and mobile operations.
- Finally, the role of command, control, communications, and intelligence (C3I) is paramount. C3I functions are seen as essential to successful implementation of such wars; consequently, the ability to interfere with an opponent's C3I functions also became much more important.[1]

The conduct of such wars would entail coordinated joint operations among forces drawn from multiple different services, operating in the same general physical area. For the PLA, "joint campaigns" within the 1990s context were defined by four criteria:

- The campaign involved two or more services;
- Each service contributed a *juntuan*-level of force, i.e., a group army, a military region air force, a fleet, a Second Artillery base;
- The campaign had a single, unified command structure; and
- The command structure developed a single, unified campaign plan, which all the participating forces were obliged to follow.[2]

By the early 2000s, having witnessed Western military operations in the Balkans and Afghanistan, the PLA shifted to preparing for "local wars under informationized conditions (*xinxihua tiaojian xia jubu zhanzheng*; 信息化条件下局部战**争**)." This change was incorporated in the 2004 Chinese white paper on national defense, but was apparently already being discussed in 1999 PLA professional military literature, and was "officially incorporated into the lexicon of the 'Military Strategic Guidelines for the New Period'" in 2002.[3]

Informationization (*xinxihua*; 信息化) is the consequence of the Information Age, and the widespread introduction of information technology. Beginning in the 1970s, the proliferation of microelectronics, computers, and telecommunications technology accelerated the ability to gather, store, manage, and transmit information. Information technology, including computers and telecommunications systems,

[1]Chinese Military Encyclopedia Committee, *Chinese Military Encyclopedia*, Vol. II (Beijing, PRC: Academy of Military Science Publishing House, July 1997), pp. 126–127.

[2]Gao Yubiao, Chief Editor, *Joint Campaign Course Materials* (Beijing, PRC: Academy of Military Science Publishing House, 2001), p. 27.

[3]David Finkelstein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,'" in Roy Kamphausen and Andrew Scobell, eds., *Right-Sizing the People's Liberation Army: Exploring the Contours of China's Military*, (Carlisle, PA: Strategic Studies Institute, 2007), p. 96.

have also permeated all aspects of society and national economies and become an integral part of a nation's infrastructure.[4]

From the Chinese perspective,

> Informationization is a comprehensive system of systems, where the broad use of information technology is the guide, where information resources are the core, where information networks are the foundation, where information industry is the support, where information talent is a key factor, where laws, policies, and standards are the safeguard.[5]

In the face of this broad trend of economic, political, and social informationization, threats to national interests and security have also become informationized. The continuing spread of information technology means that potential adversaries have unprecedented access to each others' national economies, as well as the broader population and the top decision makers. Just as the bomber and long-range missile allows an opponent to directly strike a nation without having to first break through ground or naval defenses, information technology similarly outflanks traditional military forces. Indeed, the proliferation of information technology into all aspects of society and economics makes those same aspects now more vulnerable to a range of new pressures and threats.

These threats extend beyond the information networks (e.g., vulnerability to denial-of-service attacks) and the component computers (e.g., computer viruses, malware). Instead, the very information itself can constitute a threat, if, for example, it erodes the morale of key decision makers, popular support for a conflict, or the will of the military to fight. Consequently, China's interpretation of its national interests has expanded, in step with the expanding impact of information writ large on China.

In the more traditional military sense, warfare has also become informationized. As information technology has also been incorporated into various weapons, they have become ever more precise and lethal. The networking of weapons with each other, and with sensors, allows for higher operational tempos, as night and weather conditions no longer constrain military forces as much as in the past. But informationized warfare goes beyond the incorporation of information technology into individual weapons, or even into broader systems. Rather, it is the creation of systems-of-systems, including the incorporation of information technology into every facet of military activities, e.g., logistics, intelligence collection and exploitation, and transportation, etc., that sets it apart from simply more sophisticated weapons. Indeed, one of the hallmarks of "informationized warfare" is that conflicts are not platform-vs-platform, or even system- (*xitong*; 系统) versus-system, but battles between rival arrays of systems-of-systems (*tixi*; 体系).[6]

---

[4]Tan Wenfang, "The Impact of Information Technology on Modern Psychological Warfare," *National Defense Science and Technology*, No. 5 (2009), p. 72.

[5]State Council Information Office, Tenth Five Year Plan for National Economic and Social Development, Informationization Key Point Special Plans, October 18, 2002, http://www.cia.org.cn/information/information_01_xxhgh_3.htm (accessed June 14, 2019).

[6]Bai Bangxi and Jiang Lijun, "Systems of Systems Conflict Is Not the Same as Systems Conflict," *National Defense Newspaper*, January 10, 2008.

This, in turn, has led to a modification of the concept of joint operations. Joint operations, under informationized conditions, involve integrated or unified joint operations, among forces operating across multiple domains, including the land, sea, air, outer space, and informational space domains, under a single, unified command. In this informationized environment, the distinction between forward and rear areas is blurring, as are lines separating offensive and defensive operations, or positional, mobile, and guerrilla warfare. In short, informationized warfare appears to have accelerated an evolution of joint operations, from coordinated joint operations to unified (or integrated) joint operations (*yitihua lianhe zuozhan*; 一体化联合作战) and unified strength (*yitihua liliang*; 一体化力量).[7] To use a PLA analogy, coordinated joint operations is the equivalent of "three eggs in a bowl," each egg distinct. Unified joint operations is "three eggs broken in a bowl," where the eggs intermix somewhat.[8]

Tasks and Missions for the PLA

In December 2004, Hu Jintao, in his role as chairman of the Central Military Commission, gave a major speech where he provided guidance for what the PLA should be preparing for, by charging it with a set of "historic missions for the new phase of the new century," commonly referred to as the "new historic missions."

These missions include:

- Safeguarding the role of the Chinese Communist Party (CCP). As the PLA remains a "Party army," its first responsibility is to preserve the CCP's grip on power.
- Safeguarding China's national development. As the PRC remains a developing country, it is essential that the PLA help preserve the conditions for sustaining economic development. This is especially important as the CCP considers that this is a "period of important strategic opportunity for national development"; it is therefore important the PRC capitalize on this period to develop the PRC's comprehensive national power. The PLA serves this goal by helping maintain national unity, e.g., preventing secession or other breakaway tendencies.
- Safeguarding China's expanding national interests. While the PRC may be a developing country, its expanding economic strength, as well as developments in technological trends, mean that the PLA must expand its focus beyond its traditional land frontiers.
- Safeguarding world peace.

The "new historic missions" remain in place for the PLA. Under Xi Jinping, however, the PLA itself has been massively reformed in order to better fulfill these missions as well as in order to better accommodate the evolving circumstances under which those missions must be fulfilled. Under Xi, the PLA is now preparing to undertake "informationized local wars (*xinxihua jubu zhanzheng*; 信息化局

[7]Kou Shiqiang, "A Clarification of Unified Joint Operations," *People's Liberation Army Daily*, August 11, 2004, http://www.china.com.cn/military/zhuanti/sjxjsbg/txt/2004-08/11/content_5632264.htm (accessed June 14, 2019).

[8]Yuan Wenxian, "Strengthening Communications Training in Joint Operations," *People's Liberation Army Daily*, April 9, 2002, in Foreign Broadcast Information Service .

部战**争**)," reflecting the "new circumstances" or "new conditions (*xin xingshi*; 新形势)" now confronting it.

These "new circumstances" have arisen because of a series of transformations in the broader socio-techno-economic context. These include:

- Technological transformation, rooted in big data, cloud computing, and other changes in electronic information technology;
- Industrial transformation, resulting from networking, the growth in artificial intelligence, and other elements that have elevated traditional industries to new levels;
- Military transformation, as a consequence of weapons incorporating more and more intelligence and units becoming more digitized.[9]

The result of this last transformation is a further deepening of trends that had already begun in the earlier part of this decade, including the rise of "unified joint operations (*yitihua lianhe zuozhan*; 一体化联**合作**战)" as the fundamental expression of future warfare.[10]

Of particular note is the new historic mission of "safeguarding China's expanding national interests." Chinese writings note the growing importance of the maritime, space, and electromagnetic domains for national security.[11] The "new historic missions" require that the PLA be able to establish dominance of each of these domains as a prerequisite for defending the PRC's interests. Underlying this task, in turn, is the ability to dominate the information domain, to establish "information dominance (*zhi xinxi quan*; 制信息**权**)."[12] This will have even greater urgency in light of the "new circumstances."

Establishing Information Dominance. Because all operations require information, whether about one's own forces or the adversary or the broader operational environment, only with information dominance can air, land, sea, or outer space capabilities operate to their full potential. Conversely, without information dominance, there can be no air, land, sea, or outer space dominance—and victory becomes difficult if not outright impossible. Information dominance is what supports and safeguards the other dominances.[13] PLA analysts assume that both sides will be constantly striving to achieve

[9]Ma Ting, Li Qian, and Wei Fan, "Overall Planning of the Military Electronics Industry Under the New Situation," *Journal of the China Academy of Electronic and Information Technology*, Vol. 12, No. 6 (December 2017), p. 582, and LI Chengan, *Reforming Military Education Under the New Circumstances* (Beijing, PRC: National Defense University Publishing House, 2015), p. 20.

[10]Ma, Li, and Wei, "Overall Planning of the Military Electronics Industry Under the New Situation," *Journal of the China Academy of Electronic and Information Technology* (XII, #6, December 2017), p. 582.

[11]"Military Assessment: Discussing Our Military's Historic Missions in the New Phase of the New Century," *PLA Daily*, January 9, 2006, http://mil.news.sina.com.cn/2006-01-09/0616342953.html (accessed June 14, 2018).

[12]Zheng Weiping and Liu Minfu, *Discussions on the Military's New Historic Missions* (Beijing, PRC: People's Armed Police Publishing House, 2005), p. 138.

[13]Li Yousheng, *Science of Joint Campaign Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2012), p. 69. See also pp. 69–72 for a fuller discussion of the interplay between information dominance and domination of each of these other physical domains.

information dominance, and therefore, both sides will be trying to weaken and undermine the adversary's information networks, while also trying to preserve their own.

At the same time, the proliferation of various sources of information, as well as the increasing ability to move massive amounts of data, mean that there will be more opportunities to create a common situational picture among all the participating forces. By generating such shared situational awareness, exploiting all the available information sources, Chinese analysts expect a more rapid cycling of information, allowing commanders' decisions to be more rapidly disseminated to the units, leading to a more flexible, rapid, tailored response. Command will be in real time, and operations will be promptly adaptive.

At the same time, this common situational picture would allow commanders to better track not only adversary forces, but also friendly units. This latter aspect is especially important, given the involvement of forces drawn from all the different services, who would be operating across multiple domains. As one Chinese analysis observed, even Sun-Tzu had written that only by knowing oneself as well as the adversary can one hope to be ever victorious.[14] This would be even more true in the Information Age.

This common situational picture is built upon several key pillars.

- **Real-time information.** Perhaps most important is the ability to obtain and transmit information on a real-time or near-real-time basis. Unlike in the industrial era, information systems are now sufficiently prolific that they permeate the battlefield, allowing for near-instantaneous capture of information and its transmission. Moreover, because of the advances in electronics and associated information technology, smaller, cheaper sensors can nonetheless collect and transmit enormous amounts of data. At the same time, modern warfare requires prompt access to information, because warfare under informationized conditions is both more rapid and more intense. Given the importance of establishing information dominance, it is vital that information be readily available.

- **Accurate data.** Complementing real-time availability is accuracy. In order to counter an adversary, Chinese analyses argue that it is necessary to calculate their overall combat capabilities and determine their likely courses of action, down to the individual unit level. This must include not only their equipment and manpower strength, but also their physical reach, the radius of action within a given time period, and the quality of the forces.[15] If the information necessary for such determinations is inaccurate, then the decisions that will be generated will be flawed. Similarly, the information regarding one's own forces' disposition and capabilities must not only be timely but accurate as well. Chinese assessments seem to view the greater quantity of data as leading to greater accuracy, in part because it will be collected from many

[14]Zou Zhenning and Cha Rui, *Command Information Capabilities Research, Based on Systems Combat Between Information Systems* (Beijing, PRC: Oceans Publishing House, 2011), p. 57.

[15]Sun Jinwei, *Research on Laws Governing Campaign Dilemmas and Activities* (Beijing, PRC: National Defense University Publishing House, 2013), p. 74.

different sources, including a wide array of sensors, open-source information, and cyber intelligence. Such a diverse set of sources provides a more comprehensive picture of one's own forces. It may also complicate an adversary's attempt to undertake camouflage, concealment, and deception measures (CCD), since these efforts would have to be mutually consistent to successfully fool intelligence analysts.

- **Collection of many different kinds of information for many different users.** The variety of sensors and other information sources means that information can be collected from many different domains, including the land, sea, air, outer space, and electromagnetic spectrum, to support users in not only the ground, naval, and air forces, but the political realm (for political warfare) as well. Similarly, all this information can support operations from outer space to the ocean depth, and across both an adversary's depth and one's own rear areas. Such levels of information collection are necessary, in order to maximize the effectiveness of one's own arsenal; at the same time, though, it allows commanders an unprecedented degree of situational awareness, extending for far greater distances and across a wider variety of types of information. Indeed, the collection and dissemination of information in a wide variety of forms also means that different types of information (electro-optical images, radar-generated images, electromagnetic characteristics) are all available and can be blended together to provide a more in-depth look at a target or an environment. All of this helps create a single, integrated situational picture that can then be accessed by all the participating forces, allowing everyone to have a better understanding of friendly and adversary dispositions, the overall environment, and intended operational goals and methods.

- **Intelligent information processing.** The information that is gathered, moreover, will also allow planners a very high level of efficiency, as all this information will allow for much better matching types and numbers of weapons precisely against any given target set. This will be based, in part, on the incorporation of information-processing capabilities on sensors and even weapons, so that analysts will be able to focus better on the elements that matter the most. As platforms themselves become more intelligent, it is expected that the information provided will be better tailored to the individual user, avoiding information overload despite the growth in information collected.[16]

- **Reliable communications.** One of the most essential advances allowing for the creation of a common situational picture is the advent of more secure communications. Indeed, the advances in information technology, in the Chinese view, allow not only more information to be securely transmitted, but also the greater variety, as noted previously. This increase in reliability will benefit not only command and intelligence functions, but every aspect of the joint force, including navigation, force coordination within the same echelons, and between front lines and

[16]Zou and Cha, *Command Information Capabilities Research, Based on Systems Combat Between Information Systems*, p. 61.

rear areas. As important, Chinese analysts seem to think that future communications architectures, given their networked nature and the incorporation of various security measures, will ensure that communications are safe as well.

These characteristics, in combination, will allow commanders and their subordinate forces to share information on a near-real-time basis, thereby allowing all the forces to integrate their actions. Enemy vulnerabilities can be rapidly identified, all available friendly forces can be deployed to exploit them, and strikes from a variety of locations can be coordinated to maximum effect. At the same time, better information will allow more sustained operations, preventing the adversary from regrouping while exploiting newly arising opportunities. Rather than a linear progression, operations will be able to proceed in parallel, across the depth and breadth of a theater, with precise attacks paralyzing an adversary, rather than relying upon brute force to bludgeon them into submission.[17]

From the Chinese perspective, a clear demonstration of what such information sharing can achieve was provided by the American-led coalition's operations against Iraq in the 2003 Iraq war. Because the coalition forces had superior Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance capabilities, they could forge a truly joint operational approach to the conflict, with smooth communications among the various forces. This was a significant improvement upon what had been undertaken in the Gulf War, a decade previously, where coalition ground forces had some difficulties coordinating with naval and air forces.[18]

This, in turn, requires actively undertaking offensive actions—information dominance cannot be achieved through solely defensive, reactive measures. Indeed, because of the importance of information systems to local wars under informationized conditions, as well as the nature of the information environment, "it is more important to emphasize the offensive with regards to the information domain than it is in the traditional land, sea, and air domains."[19] In particular, one needs to take sustained offensive action against the adversary's information networks, command and control infrastructure, as well as key combat forces.[20] These activities constitute the core of "information warfare (*xinxi zhan*; 信息战)."

Offensive actions are essential, as only by neutralizing the adversary can one ultimately secure one's own networks and systems-of-systems. If one's information warfare efforts are successful, the adversary's traditional combat forces will be reduced to an Industrial Age capacity. They may remain locally potent, but with only a disrupted, paralyzed, and destroyed information network, they will have only limited effectiveness.[21] In both the Gulf War and the Balkan conflict in Kosovo, the Iraqi and Serbian forces, respectively, suffered relatively few casualties, but the destruction of their "three major systems" meant that the remaining forces could not have a decisive impact. In those conflicts,

[17]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, 2nd Edition, *Campaigns* (Beijing, PRC: China Encyclopedia Publishing House, 2007), p. 127.

[18]He Zhu, *Experts Assess the Iraq War* (Beijing, PRC: Military Science Publishing House, 2004), p. 146.

[19]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 87.

[20]Wu Renhe, *Theory of Informationized Conflict* (Beijing, PRC: Military Science Publishing House, 2004), p. 168.

[21]Wang Hui, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare* (Beijing, PRC: Military Science Publishing House, 2009), p. 111.

however, the America-led coalition forces had an overwhelming set of advantages, including far more extensive information resources than the Iraqis or Serbs could field. Under more even circumstances, Chinese analyses suggest that information dominance is likely to be a more localized, temporary condition. The pervasiveness and resiliency of information networks means that it would be difficult to establish permanent information dominance. Consequently, the weaker side, by constantly and actively seeking out opportunities to concentrate their information warfare resources, can often nonetheless achieve at least local conditions of information superiority and advantage. Exploited to maximum advantage in the offensive, such local conditions can nonetheless create opportunities to paralyze the adversary and defeat them.

At the same time, whether one has achieved information dominance or not, one must also constantly undertake defensive efforts to try and preserve the integrity of one's own systems-of-systems. For the side that is technologically inferior, this will be even more difficult, as the adversary may well exploit paths and approaches that one either had not conceived of or had insufficiently prepared defenses for. Attacking the adversary's information networks must therefore be part of one's defensive efforts, even if one is weaker, both to deny the adversary the initiative and to alleviate pressure on one's own systems. It is the best means by which the weaker side can sustain an asymmetric stance that can compensate for those weaknesses and unbalance a stronger adversary.[22]

For both sides, then, whether in defense or offense, the priority targets in conducting information warfare and pursuing information dominance will include the adversary's intelligence and surveillance systems; their high technology weapons platforms and bases where they are located; their safeguarding infrastructure, systems, and forces; and their command, control, and communications networks.[23] The winner of information warfare is the side that retains a relatively more intact set of system-of-systems; in particular, the side that retains better connectivity among the various constituent systems.

Achieving "information dominance" in the face of this maelstrom of hard-kill and soft-kill weapons and tactics is not solely or even predominantly a matter of computer network attack (or defense). Instead, the Chinese conceive of information warfare at the campaign level as comprising several key lines of operations, including electronic warfare, network warfare, and space warfare.

Electronic Warfare (dianzi zhan; 电子战)

Electronic warfare is one of the earliest and most fundamental forms of information warfare. There was widespread employment of electronic warfare in the Second World War (e.g., the use of "Window" or chaff by Allied bombers to blind German air defense radars and the exploitation of cryptanalysis by all sides to outmaneuver their adversaries), and it has become increasingly sophisticated and important in the intervening decades.

Electronic warfare is the effort by each side to degrade and disrupt the adversary's electronic systems, while preserving one's own.[24] It occurs in the "electromagnetic space (*dianci kongjian*; 电磁空间),"

[22]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 87.

[23]Zhang, *The Science of Campaigns*, p. 90.

[24]Wang, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare*, p. 180.

or the electromagnetic spectrum, ranging from super low frequency to ultraviolet, including the visible light spectrum. The electromagnetic space is seen by Chinese analysts as the fifth domain of warfare, alongside land, sea, air, and outer space.[25] Indeed, electronic warfare is actually a struggle to dominate the electromagnetic spectrum, establishing electromagnetic dominance as part of the larger effort to establish information dominance.

The successful domination of the electromagnetic spectrum provides an enormous advantage in the effort to dominate the broader information space, and thereby secure the initiative, because it affects the vast majority of systems that collect, transmit, or exploit information. Electronic warfare conceptually affects radars, communications systems such as radios, as well as electronic countermeasures and electronic counter-countermeasures (ECM and ECCM) systems, as well as weapons control and guidance systems. The ability to operate successfully in the land, sea, air, or outer space will therefore be heavily influenced by the ability to operate electronics successfully. Indeed, as one Chinese assessment notes, the effort to establish the "three dominates" will be heavily influenced by the side best able to succeed at electronic warfare.[26]

Chinese analysts also argue that electronic warfare occupies a central role in modern warfare because electronics are now integrated into the very function of most weapons. Indeed, electronics have assumed a growing proportion of the cost and sophistication of modern weapons; some of the most expensive elements of modern warships or fighter planes are often embodied in the onboard electronics, rather than the metal. As one PLA analysis noted, electronics represent 20 percent of the cost of a modern warship, 24 percent of the cost of a modern armored fighting vehicle, 33 percent of a military aircraft, 45 percent of a missile, and 66 percent of a satellite.[27]

At the same time, as more and more aspects of modern warfare involve portions of the electromagnetic spectrum, the electronic environment has become much more complex. Already, current battlefields are exhibiting an increasing density of electronic systems, with both sides fielding a wide array of sensors, communications systems, and other electronic systems. Even without the two sides striving to erode the others' electronic systems, there is already an enormous amount of electromagnetic energy being emitted by the combatant forces, with the potential for mutual interference. Understanding the electromagnetic battlefield (which will likely span much greater volumes where troops are operating) is further complicated by the efforts of each side to deny the other easy access and smooth operation of their electronic systems. Not only will an enemy seek to deny easy access and smooth operation within the electromagnetic spectrum, but one's own forces and efforts may generate interference. Thus, an essential part of electronic warfare is frequency and spectrum management by the joint campaign command and reconciliation of electronic activities among the various forces, to minimize the effects of friendly emissions and those from natural sources.[28]

As the Chinese observe, some nations define electronic warfare narrowly. In the Chinese assessment, the Russians, for example, see electronic warfare as mainly involving the use of software to attack the

[25]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), p. 255.

[26]Yuan Wenxian, *The Science of Military Information* (Beijing, PRC: National Defense University Publishing House, 2007), pp. 84–85.

[27]Wang, *Foundational Knowledge, Considerations, and Explanations of Informationized Warfare*, p. 179.

[28]Yuan, *The Science of Military Information*, pp. 84 and 85.

adversary's electronic systems.[29] Similarly, a different Chinese volume concludes that the U.S. military is focused on the exploitation of the electromagnetic spectrum, both in attack and defense. In this assessment, the American approach neglects several important additional means of neutralizing an adversary's electronic systems, including

- Using either human agents or physical weapons to physically attack electronic systems;
- Using propaganda and psychological warfare techniques to degrade the effectiveness of electronic systems; or
- Using non-electromagnetic systems to counter electronic equipment.[30]

By contrast, the PLA adopts a much more expansive definition of electronic warfare. According to Chinese analyses, electronic warfare embodies the range of activities whereby one seeks to maximize the ability of one's own side to exploit the electromagnetic spectrum, while also striving to erode the adversary's ability to do the same.[31] Electronic warfare, from the Chinese perspective, therefore includes not only electronic-based weapons, but the conduct of electronic reconnaissance and counter-reconnaissance; interference and preservation measures for electronic information; and all efforts at disrupting and countering the disruption of electronic systems. Electronic warfare measures would include attacks on an adversary's communications land lines, radio networks, microwave transmission networks, and position, navigation, and timing (PNT) systems.[32] It incorporates not only soft-kill techniques, such as jamming or other forms of electronic interference and suppression, but also hard-kill approaches. The latter includes the use of artillery, aerial bombardment, and other firepower strikes to kill key kill electronic systems.

It is also important to note that, whereas electronic warfare has historically often been a tactical issue (e.g., the provision of jamming assets in support of a specific bombing raid), in the Chinese estimation electronic warfare will constitute a campaign-level activity in future local wars under informationized conditions. The proliferation of electronic warfare tools and weapons across land, sea, air, and space platforms, and the development of electronic weapons whose effects will span dozens or even hundreds of kilometers, will expand the area affected by orders of magnitude. In particular, the ability to undertake electronic warfare against space-based communications, reconnaissance, surveillance, PNT, and meteorological assets will be a vital means of establishing dominance over the electromagnetic domain.[33]

Network Warfare (wangluo zhan; 网络战)

Network warfare is the partner of electronic warfare. Also termed "network conflict (*wangluo duikang*; 网络对抗)," it is an aspect of information warfare involving the range of activities that occur

[29]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 93–94.

[30]Ye, *Science of Information Operations Teaching Materials*, pp. 21–22.

[31]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, pp. 93–94.

[32]Yuan, *The Science of Military Information*, p. 71.

[33]Ibid., p. 314.

within networked information space, as the two sides seek to reduce the effectiveness of the adversary's networks, while preserving one's own.[34] Like electronic warfare, it includes not only offensive and defensive components, but also reconnaissance of adversary and others' networks.

Network warfare occurs in the realm of "network space (*wangluo kongjian*; 网络空间)," a term that roughly parallels that of "cyberspace." However, network warfare is seen as moving beyond just computer networks, although computer network warfare remains an integral element of network warfare. In relation to information warfare at the campaign level, it occurs within networks that are part of the overall battlefield (which can extend to outer space and deep into the two sides' homelands as part of the command and control, and logistical and support infrastructures).[35]

The purpose of network warfare is to establish "network dominance (*zhi wangluo quan*; 制网络权)." When one has "network dominance," the full range of one's networks (not just computer networks) can operate smoothly and the information on those networks is safeguarded while being rapidly moved and applied, while an adversary's networks are prevented from doing the same. Some of the networks that are integral to network warfare include the command and control network, intelligence information network, and air defense network. [36] Network space is sometimes characterized as the sixth domain (alongside land, sea, air, outer space, and the electromagnetic spectrum). In some cases, however, it is seen as the fifth domain, encompassing the electromagnetic spectrum.

Because of the importance of these various networks in the conduct of unified joint operations, network warfare is considered by the Chinese as inevitably a central part of future local wars under informationized conditions. It is seen as an especially effective means for the weaker player to balance the capabilities of the stronger one. One Chinese analysis observes that in the Balkan conflicts of the 1990s, although the Serbian forces were generally outmatched by NATO, they were nonetheless able to repeatedly penetrate various NATO networks and degrade their operations. The Chinese write that the Serbs were able to penetrate the networks of the aircraft carrier USS *Theodore Roosevelt* and British Meteorological Office, affecting air operations.[37] Another Chinese analysis similarly observes that the disparities in conventional strength between NATO and Serbia were not paralleled on the Internet, where Serbian forces successfully attacked various NATO and individual member states' websites.[38]

Integrated Network and Electronic Warfare (*wangdian yiti zhan*; 网电一体战)

Of particular importance in future local wars under informationized conditions will be the steady merging of network and electronic warfare. This is the embodiment of the Chinese concept of unified joint operations. As network warfare expands and electronic warfare systems are networked, the

[34]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume) , p. 286, and Ye, *Science of Information Operations Teaching Materials*, p. 24.

[35]Ye, *Science of Information Operations Teaching Materials*, p. 28.

[36]Ibid., pp. 24 and 25.

[37]Yuan Wenxian, *Joint Campaign Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2009), p. 14.

[38]Yuan, *The Science of Military Information*, p. 73.

Chinese see network warfare and electronic warfare as inextricably linked. Indeed, Chinese military theorists were among the earliest adopters of the concept of integrated network-electronic warfare (INEW), and see INEW as a fundamental characteristic of information warfare and the informationized battlefield.[39]

The PLA defines the INEW concept (which it at times translates as "network-electronic integration warfare)" as a form of information warfare where one implements information attacks against the enemy's networked information systems through highly melded electronic warfare and network warfare."[40] It is those information warfare methods that use a combination of electronic warfare and network warfare techniques to attrit and disrupt the adversary's networked information systems, while defending one's own, in order to secure information dominance over the battlefield. It is the main expression of information warfare.[41]

As one Chinese analysis notes, in future conflicts, the electromagnetic spectrum will be the key influence upon the operation of network-space, with network and electronic warfare organically linked, operating under a single unified direction.[42] Therefore, network warfare will be affected by efforts aimed at dominating the electromagnetic spectrum, while the ability to operate electronic systems will be directly affected by efforts to penetrate and damage networks. The two elements are seen as mutually complementary in a unified effort to degrade the enemy's system-of-systems. Neither electronic warfare nor network warfare alone can comprehensively disrupt that system-of-systems, but given the mutually supporting nature of the two different types of warfare in terms of attack concepts, attack methods, and operating environments, they constitute a highly effective integrated attack methodology.

One Chinese volume observes:

> From a technical angle, electronic warfare and network warfare can be greatly complementary. Electronic warfare emphasizes attacking the signal layer, with the use of strong electromagnetic energy to drown out target signals. Network warfare emphasizes attacking the information layer, using disruptive information flow, transported into the enemy's network systems, as the means of attack.[43]

In the Chinese view, as individual facilities and their attendant information systems are networked together, the physical infrastructure upon which information passes and the information itself became an integrated whole. INEW is an effort to unify the concrete physical aspects and virtual aspects of

[39]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 101.

[40]All Army Military Terminology Management Commission, *Chinese People's Liberation Army Terminology* (Unabridged Volume), pp. 262–263.

[41]Chinese Military Encyclopedia 2nd Edition Editorial Committee, *PLA Encyclopedia*, 2nd Edition, *Military Command*, p. 327.

[42]Ye Zheng, *Concepts of Informationized Operations* (Beijing, PRC: Military Science Publishing House, 2007), p. 157, and YE Zheng, *Science of Information Operations Teaching Materials* (Beijing, PRC: Military Science Publishing House, 2013), p. 27.

[43]Ye, *Science of Information Operations Teaching Materials*, pp. 28–29.

information warfare, merging them into a single concept of operations.[44] By undertaking attacks on both of these elements, it is more likely that one can establish information dominance. INEW therefore envisions using electromagnetic attack and defense and information attack as the main techniques for degrading adversary ability to gather and exploit information, treating networked information systems as the domain of operations. Successful conduct of integrated network and electronic warfare should lead to dominance of the entire "battlefield information space (*zhanchang xinxi kongjian*; 战场信息空间)."

The central point of the Chinese conception of INEW is the incorporation of targeting (and defense) of the physical element of the information networks into network warfare. This is what makes INEW more than simply adding electronic warfare techniques to network warfare; it expands information warfare beyond the predominantly virtual world of data to include the physical, tangible world. In the context of the greater emphasis on unified joint operations, INEW is envisioned as a key example of the new kind of unified jointness necessary to successfully fight local wars under informationized conditions.[45]

Space Warfare (taikong zhan; 太空战)

As PLA writings have noted, "informationized warfare" does not simply refer to the use of computers and cyberwarfare. It involves the acquisition, transmission, and exploitation of all forms of information. Chinese writings indicate a growing recognition that space plays a central role in all these tasks. In the 2006 edition of *The Science of Campaigns*, it is specifically stated that "the space domain daily is becoming a vital battle-space…. Space has already become the new strategic high ground."[46] In the subsequent 2013 edition of *The Science of Military Strategy* from the PLA's Academy of Military Science, space is deemed the "high ground in wars under informationized conditions," tied to the struggles in network space and the electromagnetic spectrum as key future battlegrounds.[47]

In the 2015 PLA National Defense University volume also entitled *The Science of Military Strategy*, space is discussed at length, both as a new area of military conflict (alongside network space and deep ocean regions), and as an area of acquisition and development. In the first case, it is described as a key factor in the ongoing military transformation, with a major impact on future warfare's stance, form, and principles.[48] In the latter section, this is reinforced by the observation that space is the strategic "high ground" in any international military competition. "A nation's military aerospace strength will determine a nation's international standing and security."[49]

---

[44]Academy of Military Science Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, p. 101.

[45]Ye, *Science of Information Operations Teaching Materials*, p. 28.

[46]Zhang, *The Science of Campaigns*, p. 87.

[47]Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy* (Beijing, PRC: Military Science Publishing House, 2013), pp. 146–147.

[48]Xiao Tianliang, *The Science of Military Strategy* (Beijing, PRC: National Defense University Publishing House, 2015), p. 136.

[49]Ibid., p. 373.

In the Chinese conception, space is important for the advantage it confers with regards to the ability to collect, transmit, and exploit information, rather than for its own sake. As other Chinese analysts conclude, "space operations will be a core means of establishing information advantage."[50] To this end, Chinese analysts have long recognized, since at least the first Gulf War, that space is a key means of providing information support to terrestrial forces. Consequently, the emphasis upon establishing "space dominance (*zhitian quan*; 制天权)," as part of the struggle for information dominance, has become more explicit.

Several PLA analyses, for example, have observed that space is the "strategic high ground (*zhanlue zhigao dian*; 战略制高点)" in informationized warfare. They conclude that the ability to dominate space will have greater impact on informationized warfare than any other domain because it will provide:

- Real-time, global monitoring and early warning, such that no major military activity can occur without being spotted;
- Secure, long-range, intercontinental communications; and
- Positional and navigational information that will support long-range precision strike, including against targets that are over the horizon.

All of these will occur without restriction from political borders, physical geography, or weather conditions and time of day.[51]

Space dominance entails not only the ability to provide information support to the PLA, but also to deny an adversary the ability to exploit space to gain information. The American reliance on space systems, in particular, has been remarked upon. One Chinese assessment notes high levels of American investment in military communications satellites, navigation satellites, reconnaissance and surveillance satellites, ballistic missile early warning satellites, and environment monitoring satellites.[52] These satellite constellations, moreover, will be complemented by an array of terrestrial and aerial systems to provide a complete, overlapping array of surveillance capabilities. The expectation is that the United States is preparing to disrupt, degrade, deny, and destroy adversary space systems in the effort to establish information dominance; conversely, that the Americans are also preparing to face such attacks against their own systems.

Nor is American dependence upon space unique, in the Chinese view. PLA writings indicate that they are also closely observing other nations' space developments. Russian space developments, in particular, seem to garner heavy Chinese attention. The Chinese military textbook *Military Astronautics* discusses Russian as well as American aerospace forces.[53] The 2013 edition of *The Science of Military Strategy* observes that Russia has made space a major focus of its military refurbishment effort, and that Moscow has increased its investments in the space sector as the Russian

[50]Yuan, *Science of Military Information*, p. 324.

[51]Ye, *Concepts of Informationized Operations*, p. 154, and Chi Yajun and Xiao Yunhua, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing, PRC: Military Science Publishing House, 2005), pp. 38–39.

[52]Xu Guoxing, *Research on Our Military's Information Operations Strength Construction* (Beijing, PRC: Military Science Publishing House, 2013), p. 50.

[53]Chang Xianqi, *Military Astronautics*, 2nd ed., (Beijing, PRC: National Defense Industries Press, 2005), pp. 219–220.

economy has improved.[54] In particular, Russian dependence on space systems has been noted. One Chinese volume related the Russian observation that "[i]f Russia did not have an advantage in space, then it would not have reliable communications and reconnaissance, in which case, it would lack modernized information systems," leaving Russia blind and deaf.[55]

This will make the struggle for space dominance that much more pointed. If, as Chinese authors believe, without space dominance, one cannot obtain information dominance and aerial dominance, and therefore one cannot achieve land or maritime dominance, then space will inevitably be a battleground, if only in order to deny an adversary the ability to use space freely.[56] Therefore, the space arena will be one of the very first scenes of conflict, as the two sides struggle for control of space. Neither side can afford to neglect this theater, as it will be a central determinant of who will secure information dominance.[57]

Prospects for the Future

The PLA, despite being a Party army, is nonetheless a professional organization devoting substantial effort to analyzing the nature of modern conflict, in the Information Age, in order to better fulfill its "new historic missions." As important, it is modernizing its forces, based on its findings.

In light of the "new historic missions," for example, it should not be surprising that there has been a substantial effort to improve the PLA's maritime capabilities. As the 2019 Department of Defense report to Congress on China's military capabilities notes, the PLA Navy is replacing "obsolescent, generally single-purpose platforms in favor of larger, multi-role combatants featuring advanced, anti-ship, anti-air, and anti-submarine weapons and sensors." At the same time, the Chinese navy is increasingly emphasizing the maritime domain, as it now regularly conducts various missions and operations farther and farther from Chinese shores.[58] This has included indigenous construction of aircraft carriers, serial production of multiple different surface combatants and submarine classes, and the expansion of the PLA naval infantry force. This last effort, which is expected to see a tripling in size from 10,000 men organized in two brigades to 30,000 men in seven brigades, is consistent with the ongoing focus on Taiwan.[59]

Similarly, the Chinese emphasis on space dominance would suggest that the PLA would not be focused solely on information collection systems, but would also push the development of space weapons. This is also consistent with what has been observed in China's military space forces.

Under Hu Jintao, the PLA began to demonstrate overt space combat capabilities. The PLA tested its direct ascent, kinetic kill anti-satellite (ASAT) system in January 2007. Launched from Xichang

[54]Academy of Military Science Military Strategy Research Office, *The Science of Military Strategy*, p. 180.

[55]Wu Renhe, *Theory of Informationized Conflict* (Beijing, PRC: Military Science Publishing House, 2004), p. 102.

[56]Ye, *Concepts of Informationized Operations*, p. 154.

[57]Chi Yajun and Xiao Yunhua, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing, PRC: Military Science Publishing House, 2005), pp. 38 and 39.

[58]Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: Department of Defense, 2019), p. 35.

[59]Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018* (Washington, DC: Department of Defense, 2018), p. 24.

Satellite Launch Center, the Chinese ASAT destroyed a defunct Fengyun-1C weather satellite in low orbit. In the process, China also generated a massive amount of space debris.[60] Almost precisely three years later, in January 2010, China engaged in what was termed an anti-missile test, involving "two geographically separated missile launch events with an exo-atmospheric collision also being observed by space-based sensors," according to the United States Department of Defense.[61] This test also helped Chinese scientists improve their ASAT system. And in August 2010, two Chinese microsatellites were deliberately maneuvered into close proximity, and apparently "bumped" each other.[62]

These efforts at developing anti-satellite systems have been sustained under Xi Jinping. In May 2013, the Chinese conducted another anti-satellite test. This weapon, however, is assessed as demonstrating an ability to threaten targets as far as the geosynchronous belt, over 26,000 miles away.[63] This is the first time that any nation has tested a weapon explicitly intended to hold satellites in that orbit at risk. Described by one senior U.S. military officer as the "most valuable orbit," the geosynchronous region is populated by not only large numbers of communications satellites, but also strategic early warning satellites as well as weather satellites.[64] The ability to destroy such satellites would be a major step towards establishing information dominance. China conducted what it termed a missile interceptor in July 2014, but which the United States has assessed as an anti-satellite weapon.[65]

As important as the individual weapons, from the Chinese perspective, is the ability to field weapons in units, as part of a system-of-systems. In this regard, American intelligence assessments have concluded that the PLA is already employing these weapons at the unit level.[66] These units, moreover, are part of the PLA Strategic Support Force (PLASSF), a new organization created at the end of 2015 that combines China's electronic warfare, network warfare, and space warfare forces. Given the importance of these capabilities in the Chinese view for achieving "information dominance," the consolidation of the units that conduct these operations into a single service would be consistent with efforts to secure such dominance.

* * * * * * * * * * * * * * * * * * *

[60]Leonard David, "China's Antisatellite Test; Worrisome Debris Cloud Encircles Earth," Space.com, February 2, 2007, http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html (accessed June 14, 2019).

[61]"China: Missile Defense System Test Successful," *USAToday*, January 11, 2010, http://www.usatoday.com/news/world/2010-01-11-china-missile-defense_N.htm (accessed June 14, 2019).

[62]William Matthews, "Chinese Puzzle," *Defense News*, September 6, 2010, http://www.defensenews.com/story.php?i=4767907 (accessed June 14, 2019).

[63]Brian Weeden, *Through a Glass Darkly: Chinese, Russian, and American Anti-Satellite Testing in Space* (Washington, DC: Secure World Foundation, 2014).

[64]Mike Gruss, "Space Surveillance Satellites Pressed into Early Service," *Space News*, September 18, 2015, http://spacenews.com/space-surveillance-sats-pressed-into-early-service/ (accessed June 14, 2019).

[65]Mike Gruss, "U.S. State Department: China Tested Anti-Satellite Weapon," *Space News*, July 28, 2014, https://spacenews.com/41413us-state-department-china-tested-anti-satellite-weapon/ (accessed June 14, 2019).

[66]National Air and Space Intelligence Center, *Competing in Space* (Dayton, OH: NASIC, 2019), p. 21, https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf?ver=2019-01-23-150035-697 (accessed June 14, 2019).

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2016, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2016 income came from the following sources:

Individuals 75.3%
Foundations 20.3%
Corporations 1.8%
Program revenue and other income 2.6%

The top five corporate givers provided The Heritage Foundation with 1.0% of its 2016 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.