What the Chinese People’s Liberation Army Can Do to Thwart the Army’s Multi-Domain Task Force

by Larry M. Wortzel
What the Chinese People’s Liberation Army Can Do to Thwart the Army’s Multi-Domain Task Force

by Larry M. Wortzel
Land Warfare Paper No. 126, July 2019

What the Chinese People's Liberation Army Can Do to Thwart the Army’s Multi-Domain Task Force

by Larry M. Wortzel

Dr. Larry M Wortzel had a distinguished 32-year military career, retiring as an Army Colonel in 1999. A graduate of the U.S. Army War College, he earned his BA from Columbus College, Georgia, and his MA and PhD from the University of Hawaii. His last military position was the Director of the Strategic Studies Institute of the U.S. Army War College. He is currently an Adjunct Research Professor at the U.S. Army War College.

After three years in the Marine Corps and attending some college, Dr. Wortzel began his professional career assessing political and military events in China as a sergeant in the U.S. Army Security Agency in 1970 and gathering communications intelligence on Chinese military activities in Laos and Vietnam during the Vietnam War. After Infantry Officer Candidate School, Ranger and Airborne training, he was an infantry officer for four years. He moved back into military intelligence in 1977.

In the Indo–Pacific theater, he has served in the 3rd Battalion, 27th Marines; 7th Radio Research Field Station, Thailand; 1st Battalion, 9th Infantry in Korea; U.S. Pacific Command; attached to the Defense Attaché Office in Singapore; and served two tours of duty as Military Attaché at the American Embassy in China.

After retiring from the Army, Dr. Wortzel was the Asian Studies Center Director and then the Vice President at The Heritage Foundation. He has served as a commissioner on the congressionally-appointed U.S.-China Economic and Security Review Commission since 2001.
Contents

Preface ............................................................................................................................................... v
Introduction....................................................................................................................................... 1
    An Introductory Look at MDO Development in the PLA.......................................................... 2
The U.S. Army’s Road to the MDTF.............................................................................................. 3
The Strategic Support Force........................................................................................................... 3
The PLA’s Advances in EMP Weapons....................................................................................... 5
The PLA and Missiles..................................................................................................................... 5
Hypersonic Missiles on Land and in Space ................................................................................ 8
Space and PLA Capabilities........................................................................................................... 9
Unmanned Combat Platforms.......................................................................................................10
China’s Limitations .......................................................................................................................10
Conclusion......................................................................................................................................11
Notes .............................................................................................................................................13
Preface

The U.S. Army is radically changing both military culture and the conduct of operations in their incorporation of Multi-Domain Operations (MDO). U.S. Army Pacific Commander General Robert B. Brown described the Multi-Domain Task Force (MDTF) as “a significant step toward integrated, joint formations,” and declared that “we are driving the progress toward the changing nature of warfare.” The Army’s MDTF includes: a more robust incorporation of cyber and electronic warfare in various echelons of Army units; an expansion of the personnel and resources devoted to space operations; and new ways to conduct anti-ship operations from land with precision long-range fires. The concept is very different from the way that the Army approaches large-scale land warfare with major formations, fixing forces, blocking forces and decisive forces. In the Indo–Pacific theater, however, MDTF facilitates joint MDO.

This monograph briefly examines U.S. Army efforts to develop operating concepts and conduct MDO at different levels of war, then takes a more extensive look at how the People’s Liberation Army (PLA) of China has adopted the concept of multi-domain warfare and analyzes the capabilities of the PLA to counter the Army’s nascent MDTF.

The Chinese are also focused on joint, integrated operations across multiple domains of war. Tactically, the PLA has supported such efforts by strongly advancing naval force deployments and the development of new air force assets. Strategically, they have sought to employ “soft” attacks with electromagnetic energy systems, following these soft strikes with “hard” attacks. For example, cyberattacks or the use of electromagnetic pulse (EMP) weapons might precede precision-strike kinetic weapons. The PLA’s strengths are in the use of electronic warfare, cyber warfare, counter-space warfare, space surveillance and the inclusion of hypersonic weapons in their kinetic strikes.

This monograph explains the threats an MDTF may face in countering the PLA, even prior to deployment. As the Army and the other services develop force packages and operational strategies for the Indo–Pacific region, they must ensure that defenses and tactics are adequate to meet the serious threat posed by China’s hypersonic weapons, missiles, naval gunfire, air attack and sophisticated forms of cyber and electromagnetic attack.
What the Chinese People’s Liberation Army Can Do to Thwart the Army’s Multi-Domain Task Force

Introduction

This monograph briefly examines U.S. Army efforts to develop operating concepts and conduct Multi-Domain Operations (MDO) at different levels of war, then takes a more extensive look at how the People’s Liberation Army (PLA) has adopted the concept of multi-domain warfare and analyzes the capabilities of the PLA to counter the Army’s nascent Multi-Domain Task Force (MDTF).

Broadly, the U.S. Army is radically changing both military culture and the conduct of operations in their incorporation of MDO.1 U.S. Army Pacific Commander, General Robert B. Brown, described the MDTF effort to the Association of the United States Army: “The Multi-Domain Task Force pilot program is a significant step toward integrated, joint formations, and we are driving the progress toward the changing nature of warfare.”2 More specifically, the Army’s MDTF includes: a more robust incorporation of cyber and electronic warfare (EW) in various echelons of Army units; an expansion of the personnel and resources devoted to space operations; and new ways to conduct anti-ship operations from land with long-range precision fires.3

The Chinese are similarly focused on joint, integrated operations across multiple domains of war (land, sea, air, space, the electromagnetic spectrum and information). PLA doctrinal thinking has been exploring this subject for almost two decades.4 About ten years ago, it actively began to incorporate MDO into exercises and doctrine.5 Tactically, the PLA has supported such efforts by strongly advancing naval force deployments and the development of new air force assets. Strategically, they have sought to employ “soft” attacks with electromagnetic energy systems, following these soft strikes with “hard” attacks. For example, cyberattacks or the use of electromagnetic pulse (EMP) weapons might precede precision-strike kinetic weapons.6

Together with looking at the development of Chinese theories in this field, this monograph analyzes the PLA’s practical threat to the Army’s MDTF. The Army officially released the idea
of MDO in Field Manual 3.0, *Operations*, in October 2017, amending it slightly that December. According to the Modern Warfare Institute at the U.S. Military Academy, the concept was motivated by then Deputy Secretary of Defense Bob Work. In a U.S. Army War College speech, he stated, “In the future, Army and U.S. Marine forces and our allies that fight with us are going to have to fight on a battlefield that is swept by precision-guided munitions, but also one that is swept by persistent and effective cyber and EW attacks.” In this light, Mr. Work first discussed Russian military operations in the Ukraine and then turned to China: “A ground combat on the front lines is going to have to contend with what the Chinese call ‘informationalized warfare.’” In the Chinese perspective, Work explained, this is the combination of cyber, EW, information ops, deception and denial that disrupts American command and control (C2) and so gives the enemy an advantage in the decision cycle.

**An Introductory Look at MDO Development in the PLA**

Chinese strategists pay close attention to developments in U.S. military doctrine and thinking; discussion of MDO is no exception. Two researchers in particular at the PLA’s National Defense University Political College have analyzed the American concept; Liu Shuoyi and Li Bo argue that “the shift of U.S. forces from Iraq and Afghanistan toward Asia also influenced the U.S. Air-Sea Battle concept and had a strong effect on traditional Army operations under the mode of highly-informationalized operations [高度信息化的作战模式].” Overall, the PLA frames the Army’s MDO effort as another U.S. attempt to respond to and defeat China’s own counter-intervention/area denial and repel (反介入/区域拒止) strategy—one designed to keep enemy forces from intervening in a conflict near China. In response, the PLA has developed a number of practical capabilities that could stymy, or at least challenge, the MDTF. It is simultaneously developing the operational concepts necessary to guide them and to integrate them—focusing in particular on the role of integrated domains in future war—and it is ahead of the United States in advancing ideas about multi-domain warfare and in exercising forces to conduct these operations. Newly-developed and developing Chinese capabilities are summarized in the list below and are discussed in greater detail in subsequent sections of this monograph.

- **Strategic Support Force** (SSF) reforms in 2016 led to a consolidation at all levels of war for the Central Military Commission (CMC) and the PLA in areas including information operations, space operations, intelligence, surveillance and reconnaissance (ISR), EW and cyber warfare.

- **The PLA’s advances in EMP weapons**, including improved PLA navy over-the-horizon (OTH) targeting capabilities with sky wave and surface wave OTH radar, can be used with reconnaissance satellites to locate and conduct precision strikes on targets at great distances from China.

- **The PLA’s development of missiles** is happening in many arenas and poses the most significant threat to the United States.

- **Advances in hypersonic warfare** in the PLA are notable; they mean increased threats to the United States on land and in space.

- **The PLA’s increased capabilities in space** will mean more frequent interruptions of an MDTF’s ISR, positioning, navigation and timing (PNT) and similar functions.

- **Unmanned combat platforms** are also being developed and increasingly utilized by the PLA; they are effective in ISR, EW and targeting against MDTFs.
Although not discussed below, it is also important to note changes in the PLA’s rocket force; the Chinese Communist Party has reorganized the PLA and created a joint organization subordinate to the Party’s CMC. This reform, which took place in December 2015 and January 2016, saw the evolution of the second artillery corps to the PLA rocket force, a separate and independent branch of the military. It is also worth mentioning that the PLA marine corps has expanded from two brigades to six brigades and has improved special operations capabilities.

The U.S. Army’s Road to the MDTF

Army efforts to claim proficiency in MDO arguably began with an exercise on 12 February 1995, when an Army Tactical Missile System (ATACMS) was successfully fired from the deck of the USS Mount Vernon. Progress stalled after that exercise; momentum did not pick up again until October 2016. At a seminar discussing the concept of a “Third Offset,” then Secretary of Defense Ash Carter announced that the DoD Strategic Capabilities Office was exploring “integrating an existing seeker into the ATACMS, enabling it to hit moving targets, both on land and at sea.”

DoD officials acknowledge that such systems are limited by their dependence on PNT from GPS. In the future, they will need a seeker—an independent navigation system that can be attached to the front of a missile—to provide an additional way to operate in a GPS-denied area. The chances of the Army’s MDTF operating in such an environment are high—particularly if it engages in combat or pre-combat operations at a time of increased tension with China. This problem is not unique to the MDTF; the U.S. Marine Corps (USMC) will face similar challenges as it refines its own concept of multi-domain Expeditionary Amphibious Base Operations (EABO), one that involves missiles, artillery, aircraft, ISR, air defenses and cyber, EW and space support.

Some of the concepts involved in fleshing out an MDTF are not new. In Iraq and Afghanistan, the Army successfully employed cross-functional teams; they were used again in the Rim of the Pacific Exercise in the summer of 2018. At the same time, these concepts are also responsive to the need to engage with China as a potential threat. Combined-arms units of infantry, artillery (such as ATACMS), air defense, communications and ISR units such as the MDTF could help deny China’s air force and navy unfettered access through such restricted routes as the Miyako Strait, the Bashi Channel, the Lombok Strait and the Sunda Strait. Similarly, in the early stages of World War II, the first domino in Japan’s strategy to invade the Philippines was the seizure of Batan Island in the Philippine archipelago. That bolstered Japan’s efforts to control the Luzon Strait. That said, the PLA is well-equipped to counter the MDTF in such a scenario.

American military leaders acknowledge that the Army cannot dominate the land battlefield without access to, and the capacity to take advantage of, air, cyber and space domains. There is an obvious sea component too; the Army is contemplating engaging ships with long-range missiles. Moreover, forces and materiel both depend on air, naval or maritime transport. The Army has made a series of efforts to permit operations across domains, establishing Cyber Command in 2010 and dedicating resources to the Space and Missile Defense Command/U.S. Army Forces Strategic Command and the Space Brigade at Fort Peterson, Colorado.

The Strategic Support Force

The PLA has traditionally been an artillery-dominant force with good EW capabilities. Over the past two decades, moving toward the new SSF, it has refined (and implemented in
exercises) a doctrine called Integrated Network Electronic Warfare (INEW) that combines precision strike, cyberattack and EW.20

INEW is similar to the Cold War Soviet concept of radio-electronic combat (REC).21 The goals of Soviet REC were to:

- sow confusion and disrupt and paralyze enemy C2 and logistical structure;
- support expanded special operations forces against enemy rear areas;
- employ a reconnaissance-strike concept task organized across a front; and
- destroy or neutralize enemy nuclear delivery systems.

The Soviets relied on intelligence support, reconnaissance and target acquisition. They often used radio direction finding and signals intelligence to locate important C2 nodes, enemy troop and weapon concentrations. They would then combine kinetic and electronic attacks to degrade enemy forces by 60 percent. They predicted that fires or combat action would degrade 30 percent of the force, while another 30 percent would succumb to jamming and EW. The Soviets also employed deception and other electronic countermeasures to protect their own forces.22

China’s military has not openly published any such predictions for how much damage an INEW attack could inflict on an enemy. However, in their efforts to augment the new SSF, the PLA has added additional dimensions to the older, Soviet concept. Taking a cue from U.S. military operations in Iraq and the Balkans, China has elevated INEW to a strategic level of war, moving beyond the tactical and theater realm of operations. The PLA has also added cyber-attacks and attacks on satellites, or space warfare, to its offensive operations. In doing so, it expects to weaken and paralyze not only an enemy’s decisionmaking abilities but also the political, economic and military aspects of the enemy’s entire war potential. Dai Qingmin, then director of the PLA electronic warfare and radar department, envisions future combat operations focusing on “the destruction and control of the enemy’s information infrastructure and strategic life-blood, selecting key enemy targets and launching effective network-electronic attacks.”23 This suggests that while INEW operations would take place within a theater of war, they could also extend to an enemy’s homeland—targeting both the civil infrastructure and the economy.24

These updated PLA doctrines and capabilities also mean that an MDTF’s C4ISR (command, control, communications, computer, intelligence, surveillance and reconnaissance)—and, more broadly, all information related to its force deployment list and logistics—could find itself under an SSF attack even before it deployed. Jiang Yamin, a professor at China’s Academy of Military Science, writes that China must have the capability to engage an enemy at a great distance, even in its homeland.25 In a military newspaper article on attacks on knowledge networks and enemy C4ISR, Zhang Wenrong, a PLA officer, calls for “long-range damaging attacks, precision point strikes and decapitation strikes against enemy operational systems” and using precision firepower strike, saboteurs and information attack methods to implement structural damage.26 Xu Rongsheng, a senior cyber security expert at the Chinese Academy of Sciences, said in an interview, “Cyber warfare may be carried out in two ways. In wartimes, disrupt and damage the networks of infrastructure facilities, such as the power, telecommunications and education systems in a country; or, in military engagements, the cyber technology of the military forces can be turned into combat capabilities.”27 China’s history of intrusive
reconnaissance in and exploitation of U.S. cyber networks suggests that even in peacetime, MDTFs could be targets of computer network exploitation and attack. Vulnerabilities to U.S. forces can only be expected to increase with these increased capabilities of China’s SSF.

**The PLA’s Advances in EMP Weapons**

In addition to bolstering a new SSF, the PLA is also making strides to counter MDTF through the exploration of “new concept weapons” or high-technology weapons; part of this includes increasing the effectiveness of EMP weapons. Researchers at a Chinese laboratory believe that, once fielded, such weapons would change operational concepts in war and the style of operations.

In an article exploring the destructive effects of EMP, a researcher from the National Defense Science and Technology University explained that the EMP discharge from a nuclear detonation may have great destructive effect on all forms of ground-based electronic equipment, including friendly systems. He concludes that EMP effects can destroy intelligence, communications and surveillance satellites in space, but also that the detonations cannot be precisely controlled. It is likely, he argues, that newer forms of non-nuclear EMP weapons presently being developed would have the ability to wipe out an enemy’s communications and electronic infrastructure while—assuming proper defenses—leaving one’s own intact.

Four researchers at the PLA Air Force Early Warning Academy suggested that a high-power microwave (HPM) bomb produces a directed energy with EMP-like effects, but in a more controllable form. At a PLA electronic engineering institute, researchers have used computer modeling to calculate the degree of damage that an HPM bomb detonated in an oblique attitude might cause to computers. They found that the degree hinges on four chief factors: the power of the bomb; the attitude and ellipse that the detonation creates on the ground; the orientation of any target antennas; and interference in the target area.

A 2015 Chinese article in *The Journal of Ship Research* explored the lethality of both HPM and EMP weapons. The authors cite the United States using non-nuclear EMP weapons during the war in Kosovo in 1999 and Russian experimentation in the use of HPM weapons. They argue that, given the state of development in other countries, “China must conduct deep research into the technologies” as well as into defensive measures and shielding measures.

Three researchers from the PLA Air Force Engineering Institute believe that future warfare will likely involve EMP weapons, HPM weapons and high-altitude EMP weapons. The amount of research on the topic in China and the discussions of effects in PLA literature suggest that EMP can be expected to play a role if conflict breaks out between the U.S. and China; any deployed MDTF would face some form of EMP attack. Such attacks can devastate electronic equipment. But their decisive effect in war hinges on follow-up: are they succeeded by kinetic tools that blow up and kill people? For such attacks, the PLA prefers missile delivery.

**The PLA and Missiles**

Generally speaking, the PLA air force and naval air force have improved bomber and ground-attack capabilities with cooperative target engagement capabilities and land attack missiles, including tactical air-to-surface missiles (ASM) and precision-guided munitions such as all-weather, satellite-guided bombs, anti-radiation missiles and laser-guided bombs. Their advancements have happened in missiles of all ranges:
• short-range ballistic missiles (SRBMs with ranges of 300–1,000 km) in the PLA rocket force, which now has approximately 1,200 SRBMs;

• approximately 200–300 conventional medium-range ballistic missiles (MRBMs with ranges of 1,000–3,000 km) fielded by the PLA to increase the range for precision strikes against land targets and naval ships operating out to and beyond the “first island chain”; and

• a series of nuclear and conventional intermediate-range ballistic missiles (IRBMs 3,000–5,500 km) fielded by the rocket force that are road-mobile and increase the capability for near-precision strike as far as the “second island chain.”

The People’s Republic of China (PRC) would unquestionably view a deployed (or deploying) Army MDTF during a period of tension or conflict as an intervention; the PLA’s area control and counter-intervention strategy seeks to degrade the opponent’s technical and weapon advantages and to control maritime approaches to China—or, at a minimum, to deny the enemy full freedom of action in maritime approaches to China. The PLA response to such an intervention would likely begin with soft attacks that paved the way for hard attacks. Initial (soft) attacks would include a suite of EW and counter-reconnaissance assets to neutralize enemy missile sensor and anti-missile systems, as well as to interfere with the adversary’s C4ISR architecture. This would pave the way for kinetic—likely missile—deployment.

The PLA’s doctrine on the use of missiles in warfare and their integration with cyber and EW draws from and builds on both Soviet and American doctrine. In their seminal work, Guided Missile Combat and High Technology Wars, a group of Chinese authors point out, “The combat power of missiles is very high, but they must be used on enemy troop concentrations, important bases or facilities or other C2 nerve centers in a sudden attack by concentrated fires.” They note that, in the first Gulf War, “Iraq fired 81 Scud missiles but failed to produce serious casualties or to affect battlefield operations in a significant way. Therefore, Iraq failed to take advantage of either the killing power of missiles or their psychological effect on operations.” In this same work, these authors make an early call for better PLA precision-strike capabilities based on good ISR, telling PLA leaders that for missiles to be effective in war, they must be both accurate and massed on critical targets.

At the 2018 Zhuhai Air Show, the PRC showed off a model of the CM-401 anti-ship cruise missile (ASCM), manufactured by China Aerospace Science and Industry Corporation.
The CASIC brochure described the CM-401 as the world’s first “ultra-fast ASBM [anti-ship ballistic missile].” That claim may not be wholly true, as Russia developed a hypersonic ASCM much earlier. Still, the development of CM-401 represents a major achievement for China and a significant threat to U.S. warships. And, CM-401 is also capable of land attack.

Focusing on ballistic missiles, the PLA first modified Dong Feng (东风) 21 (DF-21), a two-stage, road-mobile, solid-fueled MRBM, to carry a warhead supported by sensor systems that are designed to track moving ships at sea. The missile has been in service since about 1991 and has several variants. It can carry both conventional and nuclear warheads and it has a range of about 900–1000 miles. The ASBM variant, Dong Feng 21D, is called the “carrier killer”; it
was developed with the specific intent of attacking large ships, like aircraft carriers, at extended ranges from China.\textsuperscript{47}

Their ballistic missile with a greater range, the Dong Feng 26 (DF-26), can also carry conventional or nuclear warheads.\textsuperscript{48} An IRBM, most analysts describe it as a longer-ranged version of the DF-21.\textsuperscript{49} The DF-26 is considered China’s first conventionally-armed ballistic missile capable of striking Guam. With a range of 3,000–4,000 km, the DF-26 brings most U.S. military bases in the eastern Pacific Ocean into range from China. Like the DF-21, the DF-26 may have a variant armed with an anti-ship warhead, although that variant may not yet be fielded.\textsuperscript{50}

In addition to the missiles, which in themselves are potent, the PLA has been developing both maneuvering reentry vehicle warheads with their own propulsion and seeker systems and maneuvering hypersonic warheads for these missiles.\textsuperscript{51} Beijing sees hypersonic weapons as asymmetric “assassin’s mace weapons”; doctrinally, they appear to be China’s choice in threatening the U.S. military and its Asia bases. The PLA tested its DF-26 ballistic missile on 27 January 2019.\textsuperscript{52} In publicizing the test, one of China’s Communist Party-controlled newspapers classified it as the test of a nuclear or conventional strike/anti-ship missile using a hypersonic gliding warhead.\textsuperscript{53} The article also claimed that China’s was the world’s first supersonic mid-range and long-range missile with boost-gliding technology. Hypersonic weaponry is discussed in greater detail below.

**Hypersonic Missiles on Land and in Space**

In August 2018, the *Washington Free Beacon* reported that China had conducted a flight test of a new hypersonic warhead. The Xingkong 2 (or Starry Sky 2) missile is multi-stage and capable of maneuvers at speeds of Mach 5.5, with a top speed of Mach 6 (4,603 miles per hour).\textsuperscript{54} Six months before the August test, the same newspaper reported the testing of a hypersonic glide vehicle (HGV), the DF-ZF, also known as the WU-14.\textsuperscript{55} This missile warhead glides near its target in near space and can maneuver during reentry, confounding U.S. defenses. The WU-14 is capable of maneuvering at speeds of between Mach 5 and Mach 10, or between 3,836 miles per hour and 7,672 miles per hour.

China’s test of the WU-14 came after the United States had tested its own hypersonic missile design from an Ohio-class submarine, indicating that PLA development and testing of new capabilities is motivated by competition.\textsuperscript{56} The challenge of hypersonic maneuvering reentry vehicles complicates MDTF deployment. Right now, the U.S. lacks systems to defend against hypersonic missiles and warheads. The PLA’s development of land attack cruise missiles and ASCMs exacerbates this defense challenge.

Naturally, then, these hypersonic developments mark a direct threat. U.S. Undersecretary of Defense for Research and Engineering, Michael Griffin, told reporters in July 2018 that it would be a mistake to cede ground to U.S. adversaries in the competition to develop hypersonic weapons.\textsuperscript{57} According to Griffin, hypersonic missiles require a “very quick response; their high speed and high maneuverability make them difficult to find and difficult to kill.”\textsuperscript{58} Griffin argues, “A space-based hypersonic defense is not a practical approach. . . . Even if you had space-based interceptors, it would be technically the wrong way to do it.” According to Griffin, “Satellites and space surveillance serve for indications of warning, the launch detection, the surveillance, acquisition, tracking—the whole arena of persistent global timely awareness.”\textsuperscript{59}
Such space-based surveillance and sensors underpin China’s approach to directing its missiles. China boasts arrays of space sensors that can work with OTH radars and other air or ship-based sensors to find targets for ASCMs and HGVs. Therefore, any conflict in which hypersonic weapons come into play would likely spread to space.

The speed and accuracy of hypersonic warheads threaten new U.S. concepts for military operations in the Pacific—including the U.S. Army’s concept of an MDTF, the USMC’s EABO and the U.S. Air Force’s concept for the distribution of forces throughout a theater of operations. The threat of hypersonic warheads demands a protective response; to that end, a combination of passive measures like high mobility, deception, electromagnetic signature reduction or emissions control and camouflage can help defend a deployed unit. However, active measures like jamming and other electronic countermeasures also have great application.

HPM weapons, particle beam weapons and laser weapons are among the technologies that can address the hypersonic threat. Adequate defenses are possible if combined with forms of cooperative target engagement. But these systems remain in the development phase. When the weapon systems are more mature, they could be combined with artificial intelligence and new fire control systems to create better defenses. It is also important to note that because these weapons demand tremendous electrical power, land-based and ship-based systems will probably be available before airborne systems. Commenting on these developments in May 2019, Lieutenant General Neil Thurgood, Director for Hypersonics, Directed Energy, Space and Rapid Acquisition for the Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology), said that while the Army is pursuing laser weapons, countering swarms of incoming warheads with them would be an inefficient and expensive use of such a capability.

**Space and PLA Capabilities**

Both the United States and China depend on space assets for ISR as well as PNT. The PLA believes that because U.S. forces operating in the Pacific depend on external lines of communication over great distances, China has an advantage if space assets come under attack. In short, the closer to China any conflict takes place, the easier it is for the PRC to use land-based, ship-based or airborne assets for ISR and targeting. However, most maneuvering reentry vehicles and cruise missiles depend on space-based PNT, even if they have some form of terminal seeker. That means that any U.S.-China conflict would likely spread to space. Testifying before the U.S.-China Economic and Security Review Commission, Mark Stokes recently noted:

Space-based assets would serve as a critical component of a broader C4ISR architecture. China is fielding increasingly sophisticated electro-optical, synthetic aperture radar, and electronic reconnaissance capabilities. Additional data relay satellite systems or the expansion of ground stations abroad could further improve China’s near-real-time targeting capability. The PLA also has been modernizing its satellite communications infrastructure, space-based survey, mapping, and navigation systems, and an increasingly diverse range of space launch vehicles.

The U.S. C4ISR architecture is equally dependent on space. China already has an impressive array of kinetic and directed energy weapons designed to attack or degrade an enemy’s space-based assets, meaning that any MDTF moving against them would likely find itself with degraded PNT and interrupted C4ISR.

One of the elements in the Army’s MDTF is likely to be a unit that can engage in space warfare as well as address the other challenges posed by the PLA. General Robert B. Brown,
Commander of U.S. Army Pacific, explains that in his view the PLA prefers “to seek advantage in the overall conflict, spanning in seven domains: land, sea, air, space, cyberspace, the electromagnetic spectrum, and psychological [warfare].” He understands that “China is also concerned with keeping conflict away from its fruitful coastal economic centers.” He outlines the “brain” of the MDTF, “the Intelligence, Information, Cyber, Electronic Warfare, and Space” detachment, i.e., the I2CEWS.56

Right now, discussion of the I2CEWS seems to point toward a battalion-sized unit.67 This is analogous to the USMC’s Marine Information Group, which is a similar organization that includes C2 communications.68 To be successful, the Army MDTF must integrate this I2CEWS with its other C2 organizations and architecture.

Unmanned Combat Platforms

The modern PLA may also be moving ahead of the United States as it advances in deploying forms of unmanned combat platforms.69 Three PLA operations experts writing in China’s Military Strategy offered a sophisticated discussion in 2018 of how the PLA would use unmanned combat platforms in land operations.70 Yan Zhensheng and Zhang Xuehui from the PLA National Defense University joint operations department and Liu Yuping from the operations department of the Northern Theater Command explained how unmanned combat platforms can be used for reconnaissance, sensor platforms, EW platforms, target designation for precision fires or for suicide vehicles (自杀式) along with manned combat formations. They also envision PLA ground forces employing swarms of unmanned aerial vehicles and ground vehicles for these purposes. Yan, Zhang and Liu also point out that in high-technology information warfare, such unmanned platforms could assist in C2 and battlefield awareness. These unmanned platforms could either conduct reconnaissance or use EW to attack a deployed MDTF, even during training deployments in peacetime or in periods of tension short of war.

Unmanned aerial vehicles (UAVs) are also utilizing some of the smaller missiles that are being developed, such as the AR-1, the HJ-10 anti-tank, the Blue Arrow 7 laser-guided, the KD-2 and also the GPS-guided munitions such as the FT-5 and LS-6, which are similar to the U.S. joint direct attack munitions.71

These threats are all real, and they must be considered in U.S. planning and projection. However, although the PLA may appear intimidating in this and other arenas, it is not a “10-foot-tall giant.” Chinese armed forces have a number of serious limitations.

China’s Limitations

Although the PLA has been exploring the concepts and doctrine for MDO for some time, at the operational level PLA units and leaders struggle to adapt to such ideas.

At the 19th Congress of the Chinese Communist Party, CMC Chairman Xi Jinping set out a series of long-term goals for the PLA.72 Reviewing the reforms made to its organization in 2015 and 2016, Xi charged it with upgrading military capabilities; he tasked the PLA with achieving basic mechanization, making substantial progress toward the application of information technologies and improving strategic capabilities by 2020. For 2035, Xi challenged the PLA to modernize military theory, its organizational structure, its personnel and also to improve weaponry. The PLA was to become a “fully-transformed, world-class force” by the mid-21st century.

However, it has experienced a number of problems. Military publications since 2015 have complained about a military where “some cadre cannot 1) judge the battlefield situation; 2)
understand the intent of senior leaders; 3) make operational decisions; 4) deploy troops properly [on the battlefield]; or 5) deal with unexpected situations. Published in the PLA’s official newspaper, PLA parlance has dubbed these the “five incapables [五个不会].” An additional term further demonstrates Xi Jinping’s critique of PLA capabilities: the “two insufficient abilities [两个能力不够]” refers to the PLA’s inability to fight and to the inability of cadre at all levels to command modern wars.

As late as 2017, in a PLA Daily critique, one author reminded the leaders of the PLA that CMC Chairman Xi Jinping maintained that “technology is the core of combat effectiveness in modern warfare [科技是现代战争的核心战斗力].” The author insisted that the military revolution has entered a critical period, that after 200 “Long Stride [跨越]” and “Firepower Strike [火力]” exercises, PLA commanders still had not eliminated the problems of the two insufficient abilities and the five incapables. Thus, even after a long period of high-intensity training for the PLA, there does not seem to be much improvement in the ability of their commanders and soldiers to operate on the modern battlefield.

It is clear, then, that while the PLA understands multi-domain warfare conceptually and has a robust doctrine for these forms of operations, it is stymied in attempts to apply such operations in practical scenarios. However, as previously discussed, one area where the PLA seems to excel is in the use of missiles, especially in conjunction with hypersonic warheads.

Conclusion

Among the ways for the U.S. Army to respond to the threats from the PLA are passive defensive measures like high mobility, deception, electromagnetic signature reduction or emissions control, the use of frequency hopping radios, multi-channel and high-frequency communications and camouflage, all of which can help protect a deployed unit. Measures like mobility, camouflage, deception and well dug-in forces can sustain military operations for extended periods of time. Also, active non-kinetic measures like jamming and other electronic counter-measures have great application. These measures alone, however, may not suffice in today’s security environment.

Addressing offensive measures in space, Air Force officials acknowledge that the United States at some point will need to take offensive action. Air Force Chief of Staff General David Goldfein said in an April 2019 speech in Colorado Springs, “It’s not enough to step into the ring and just bob and weave, block and parry, and absorb punches. At some point we’ve got to hit back.” The timing and form of such offensive action in space, however, will probably not be up to a uniformed commander; given the escalatory nature of such actions, it will likely be defined and directed at the national level. For China, the same level of national control of space offensive actions is likely; however, the PRC tends toward acting first to maximize the effect and to open avenues for other kinetic attacks.

In countering UA Vs, the services are exploring systems to “detect and counter drones.” Approaches range from “interdiction through radio-frequency jamming, spoofing of the communications links, or the more direct approach through directed-energy weapons that destroy part of the drone.” Most of the systems are hand-held and, for the scale and size needed for drones, are available now.

The biggest issue now is that deployed forces like the MDTF lack technologies that can address the hypersonic threats discussed above. As noted, these systems in the United States
are only in the development phase; once developed, combination with artificial intelligence, advanced target recognition means and new fire control systems could offer increased protection. And, again, because of the electricity they will require, their use will be more attainable and available through land- and ship-based systems before being available in airborne systems.

Critical to U.S. threat evaluation is the PRC CMC’s calculus about the likelihood of vertical escalation to nuclear exchanges, as well as horizontal escalation. The Chinese leadership prefers limited or localized conflict. But China seems to calculate that it is able to absorb losses and even nuclear strikes with less catastrophic effects than the United States could. This judgment is a function of China’s historical military culture, geography and an intentional state-directed policy of civil defense and risk distribution. This means that Chinese leaders may miscalculate American will and mistakenly take risky actions.

The PLA’s propensity to mass missile fires, use drone swarms and use missiles decisively with surprise creates a situation that could easily escalate. The ambiguity over what form any ballistic (or cruise) missile attack might take creates a volatile situation in case of any crisis over Taiwan, or between China and Japan or China and the Philippines. Adding to potential volatility is the possibility that China has between two and three times the numbers of nuclear missiles that the United States estimates. In May 2019, Defense Intelligence Agency Director Robert Ashley said that China is likely to double its nuclear stockpile over the next decade. The way that the PLA handles its commitment to dominating space and its commitment to being capable of attacking American C4ISR systems affects U.S. strategic warning, missile defenses and C2.

Despite what may be a U.S. lead in research and testing, China has hypersonic ASCMs now. China also has a robust inventory of ballistic missiles, many of which can be quickly adapted to use hypersonic warheads. Like the United States, the PRC also has a well-developed space surveillance system and an OTH radar system that will support the use of HGVs. For the United States, developing long-range cruise missiles for surface attack and stealth long-range strike UAVs would improve force capability.

All of this means that Congress should be aware of the threat from China, gauge its authorizations and appropriations accordingly, and, along with DoD, prioritize development of both defenses and hypersonic systems consonant with the priority given to Asia and the Indo–Pacific region in U.S. strategy. The services, meanwhile, as they develop force packages and operational strategies for the Indo–Pacific region, must ensure that defenses and tactics are adequate to meet the serious threat posed by China’s hypersonic weapons, missiles, naval gunfire, air attack and sophisticated forms of cyber and electromagnetic attack.
Notes


4 Qiao Liang (乔良) and Wang Xiangsui (王湘穗), Unrestricted Warfare (超限战) (Beijing: PLA Arts and Science Press, 1999); Cai Fengzhen (蔡凤震) et al., The Study of Integrated Aerospace Operations (空天一体作战学) (Beijing, China: PLA Press, 2006); Li Rongchang (李荣常) et al., Integrated, Informationalized Aerospace Operations (空天一体信息作) (Beijing, China: Military Science Publishing House, 2003); Shen Weiguang (沈伟光) et al., with Lieutenant General Li Jijun (李际均), China’s Information Warfare (中国信息战) (Beijing: China Xinhua Press, 2005), 23.


7 Despite the fact that the manual is restricted in distribution and cannot be accessed by the public directly on the Army’s website, it has been published by the Federation of American Scientists: Department of the Army, Army Doctrine Publication (ADP) 3-0, Operations (Washington, DC: U.S. Government Printing Office, 6 December 2017), https://fas.org/irp/doddir/army/fm3-0.pdf.


22 Glantz, Soviet Military Operational Art, 99–158; Chizum, Soviet Radioelectronic Combat.


32 Zhang Jinghui (张璟珲) and He Jun (何俊), “A Damage Probability Analysis of a High-Power Microwave Bomb Attacking a Computer Device by an Oblique Attitude [倾斜攻击计算机设备的毁伤能力分析],” Journal of the PLA University of Science and Technology–Natural Sciences Edition (解放军理工大学雪豹自然科学版) 17, no. 3 (June 2016): 227–232.


36 The “first island chain” in PLA parlance is the chain of major islands and archipelagos from China’s continental mainland coast out to the Pacific. Among the features are the Kuril Islands, the Japanese archipelago, the Ryukyu Islands, Taiwan, the Northern Philippines and Borneo, roughly extending from Russia’s Kamchatka Peninsula to the Malay Peninsula. See “The People’s Liberation Navy and Offshore Defense,” Global Security, accessed 16 December 2018, https://www.globalsecurity.org/military/world/china/plan-doctrine-offshore.htm.

37 Ibid. The “second island chain” includes the Japan Sea, the Philippine Sea and the Indonesia Sea, the Kuriles, Hokkaido and the Japanese Islands, Guam, the Marianas and Palau Islands.


41 Ballistic Missile Battles in High Technology Warfare, 11.


43 Known as the 3k22, the Russian BrahMos II hypersonic missile system was first tested in 2011. It has also been sold to India. A newer Russian hypersonic ASCM, the Zircon, may be a domestic version of the BrahMos II; Kyle Mizokami, “Russia’s New Hypersonic Missile Travels Nearly Two Miles a Second,” Popular Mechanics, 26 December 2018, https://www.popularmechanics.com/military/research/a25684396/zircon-hypersonic-missile/).


Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, DC: DoD, 2011). At the 2018 Zhuhai Air Show, the China Academy of Launch Vehicle Technology offered an export version of the DF-21D ASBM, the M-20B ASBM, on the international market. With a range limited to 280 km, that model adheres to the Missile Technology Control Regime—China’s arms sales history suggests that it could make its way to Pakistan and Iran; Shukla, “China’s New ‘Aircraft Carrier Killer’ Missile.”


Ibid. See also “Missile Threat, the Dong Feng 26 (DF-26),” *CSIS Missile Defense Project*, https://missilethreat.csis.org/missile/dong-feng-26-df-26/.


Mehta, “3 Thoughts on Hypersonic Weapons from the Pentagon’s Technology Chief.”


63 James R. Holmes, “China’s Way of Naval War: Mahan’s Logic, Mao’s Grammar.”


The Chinese characters for the five incapables are: 不会判断战场形势; 不会理解上级意图; 不会定下作战决心; 不会摆兵布阵; and 不会处置突发情况.


One example is the Battle of Ie Shima in World War II, where, despite heavy bombardment, Japanese forces managed to defend the island for a week: “The Capture of Ie Shima,” https://history.army.mil/books/wwii/okinawa/chapter7.htm.

Valerie Insinna, “At some point we’ve got to hit back,” Defense News 34, no. 7 (22 April 2019): 22.


The level of tolerance for the risk of nuclear war is explored in Xiao Xingbo (晓兴博), People’s Air Defense and Nuclear War (核战争与人防) (Beijing: People’s Liberation Army Press, 1989); Questions of preparations, civil defense and nuclear calculus can also be found in Zhu Mingquan (朱明泉), Nuclear Proliferation: Danger and Prevention (核扩散：危险与防止) (Shanghai: Science and Technology Literature Press, 1995) and in Yao Yunzhu (姚云竹), Post-War American Deterrence Theories and Policies (战后美国威慑理论与政策) (Beijing: National Defense University Press, 1998).


