Operational Environment & Threat Analysis

Red Diamond

Special Edition 2021

China as a Pacing Threat

Chinese Approaches to Unmanned Aircraft Systems

Chinese Information Operations

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

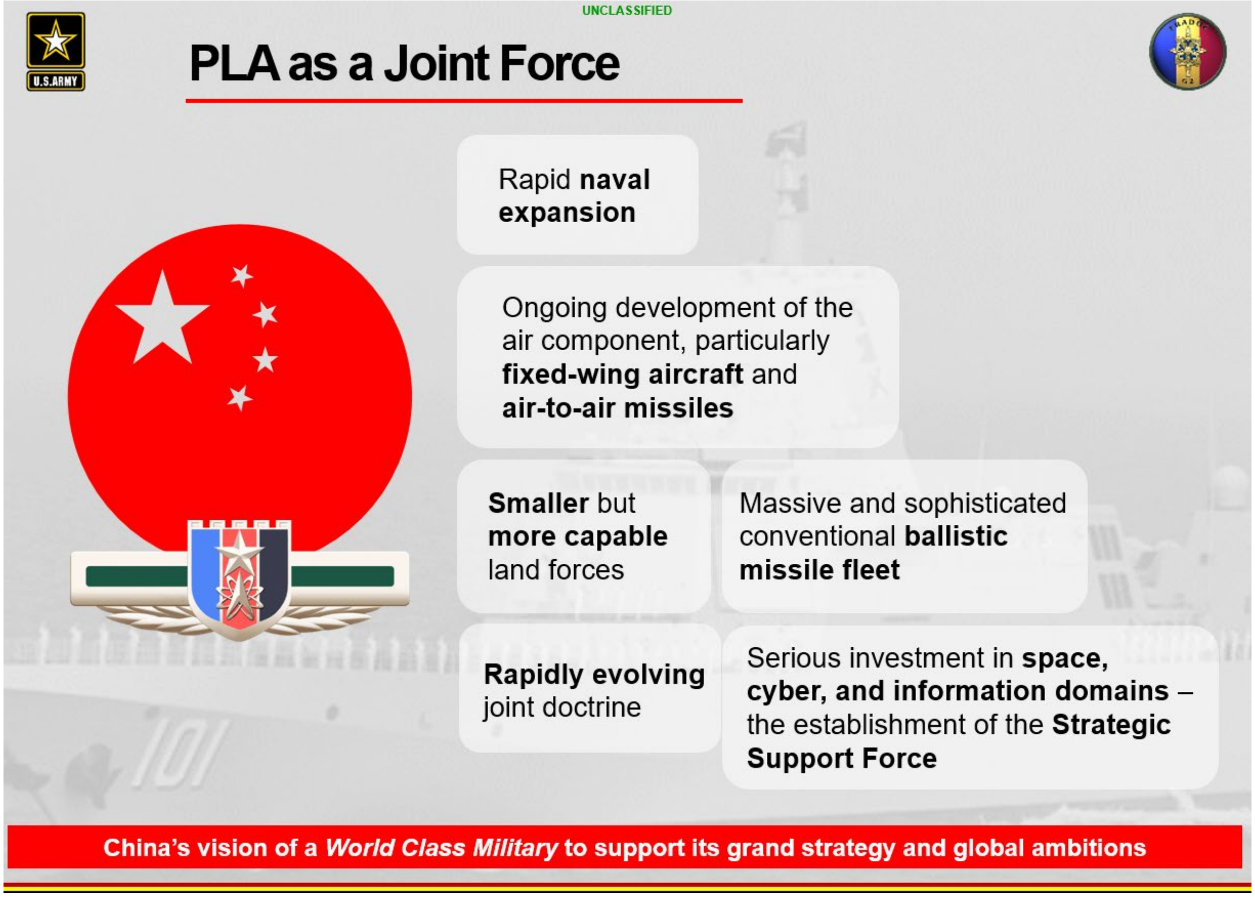
Introduction to Red Diamond Special Edition: China

China is a rapidly modernizing, nuclear-armed nation that harbors global ambitions and is increasingly active across the diplomatic, information, military, and economic spheres. It has become increasingly active in the Competition space, and it is rapidly developing capabilities designed to challenge the United States in the Crisis and Conflict spaces. Its People's Liberation Army (PLA) is undergoing a dramatic modernization effort that touches all elements of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). China has become our pacing challenge.

- The Interim National Strategic Security Guidance, published in March 2021, states that China "is the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system."
- Additionally, there is clear guidance from Army senior leaders. In June of this year, the Chief of Staff of the Army, GEN James McConville, declared that "[t]he Army must understand the threat posed by China to the same level that we understood the Soviets."
- Then in August 2021, USARPAC Commander GEN Charles Flynn offered these comments: "I reinforce to my Theater Army team here that we are singularly responsible to the INDOPACOM Commander for the PLA Ground order of battle [OOB]... but it doesn't change the fact that we have a long, long way to go to develop the institutional levels of knowledge, understanding, and expertise we require to address the wicked problem the threat poses for the Nation."

This issue of the Red Diamond presents articles and content focused on China. The majority of the content stems from existing TRADOC G-2 products, including the *Army Techniques Publication (ATP) 7-100.3: Chinese Tactics* and *The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict*. Our goal is to make this content widely accessible to the Force. TRADOC G-2's role in understanding China is to develop content that enables soldiers at all echelons to gain the greatest possible understanding of the threat across Competition, Crisis, and Conflict. Please reach out to let us know how our offerings help you or if you need something you have not found. What you need may be coming soon as we have several projects in development.

Figure 1 comes from TRADOC G-2's leader professional development presentation on the China ATP, which highlights China's concept of what it means to be a world class military. According to the 2019 Chinese Defense White Paper, the goals of China's National Defense are to create a mechanized force by 2020, a fully modernized military by 2035, and a "world class" military by 2050. The slide lists the ways in which China is modeling the PLA after best practices of both the United States and Russia, while also being innovative and implementing its own unique ideas. Note, for example, the symbol on the left of the slide, which is the unit crest for the PLA Strategic Support Forces (SSF). The SSF is a unique force created by China to implement information operations, cyber-attacks, space and counter-space operations, and kinetic and non-kinetic electronic warfare. The creation of the SSF is just one example of China's ability to innovate in its efforts to create a force capable of meeting its goals of becoming a world class military. ***(Please contact us if you would like to read our classified information paper on China's SSF – available on JWICS.)***



UNCLASSIFIED

PLA as a Joint Force

Rapid **naval expansion**

Ongoing development of the air component, particularly **fixed-wing aircraft** and **air-to-air missiles**

Smaller but **more capable** land forces

Massive and sophisticated conventional **ballistic missile fleet**

Rapidly evolving joint doctrine

Serious investment in **space, cyber, and information domains** – the establishment of the **Strategic Support Force**

China's vision of a *World Class Military* to support its grand strategy and global ambitions

Figure 1.

"The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict is accessible at: The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict – OE TRADOC (army.mil)

ATP 7-100.3: Chinese Tactics is accessible at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33195-ATP_7-100.3-000-WEB-1.pdf.

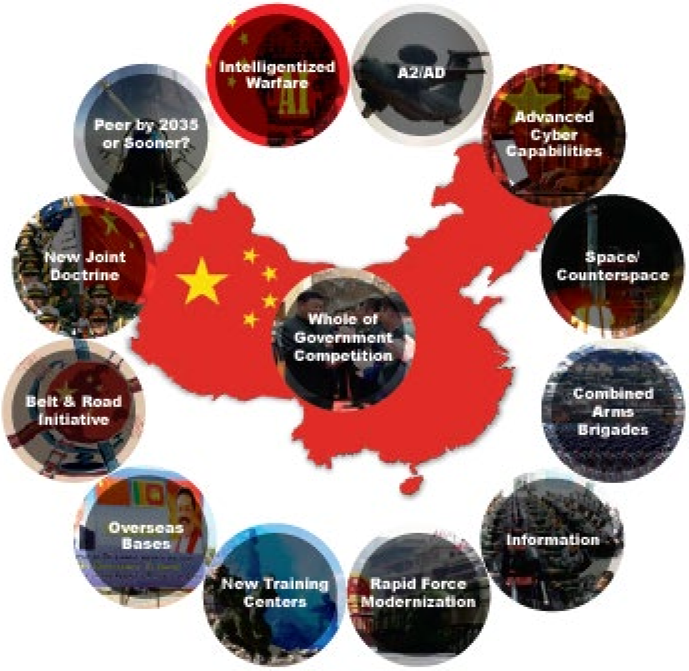
We currently offer Leader Professional Development sessions covering the content of *ATP 7-100.3* on Thursdays at 1300-1500 CDT on Microsoft Teams at this link below. You can also find other related materials at the link by accessing the Files tab. https://dod.teams.microsoft.us/l/channel/19%3adod%3a9c5460eb13584c5399ccdcf565ec6e8e%40thread.skype/General?groupId=125d8eed-1932-47c2-87f1-86ee44557693&tenantId=fae6d70f-954b-4811-92b6-0530d6f84c43.

Article 1: So Why Do We Consider China to Be Our Pacing Threat?

An excerpt from The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict

In the Introduction, we discussed how China is a rapidly modernizing, nuclear-armed nation that is on a trajectory to become a peer power to the United States. China is now our pacing threat in large part because it is our most technologically sophisticated adversary and effectively uses its economic clout and information operations to bolster its regional and increasingly global position at the expense of its adversaries. Although China’s People’s Liberation Army (PLA) lacks combat experience, it is a formidable force that is working diligently to introduce new capabilities and improve its training and leader development. In this article we will examine China’s rise in greater detail.

China wishes to prevail in the Competition or Crisis phase through the integrated use of its national power across the Diplomatic, Information, Military, and Economic (DIME) arena. China wishes to reach its desired ends by winning without fighting, and is prepared to use all instruments of national power to cause dissention among the American people, separate America from its allies and partners, and challenge American military advantage. If Crisis shifts to Conflict, Beijing hopes to win the first battle as overwhelmingly as possible, ensuring that an opponent has no desire for a second battle. China will contest us in all domains in Competition, Crisis, and Conflict, and its nuclear deterrent provides a factor that U.S. defense planning has not had to truly consider since the Cold War. The vast distances required to move a CONUS-based U.S. force to the so-called Chinese First Island Chain present a host of logistical and organizational challenges. China’s long-range precision weapons, as well as sensors and systems that can track and engage U.S. forces in all domains, exacerbate these challenges.



Source: U.S. Army TRADOC G-2

Beijing understood that its continued rise would lead to an outright rivalry and perhaps even an adversarial relationship with the United States and its Allies and partners. As a result, China began studying the U.S. approach to warfare and began broad modernization efforts to challenge the post-Cold War U.S. dominance.

China’s most recent sweeping approach to military modernization began in 2015. China is investing heavily in force modernization, and just like the United States, it is focused on key emerging technologies. Looking out to 2028, there likely will be a rough general technological equivalency between the United States and China, with both nations having relative advantages in some areas and disadvantages in others.

A great deal of attention is focused on China's material progress, which provides it overmatch capabilities under certain conditions or in niche areas. The PLA has some fires systems that outrange our own; it has highly capable EW systems; and it has developed sophisticated integrated air defense systems. At the same time, we stripped many of these capabilities from our force due to the demands of counterinsurgency. Moving forward, China is focusing on cutting-edge technologies, such as artificial intelligence, quantum computing, hypersonics, and robotics to extend its ability to challenge us in multiple domains. This directly challenges the belief that the U.S. Army has superior equipment because China's equipment is as good as ours, and in some cases better.

China's progress in modernization goes well beyond the materiel realm as it is also working to challenge us in the human capital dimension. New equipment will facilitate the effort, but if China is to defeat the United States, it recognizes the PLA will need well-trained soldiers and dynamic, thoughtful leaders. China has worked to modernize its training and instill a new culture of learning in its forces. It has established combat training centers similar to our own. It has also professionalized its leadership development efforts and is working to develop professional military education programs that cultivate more agile leaders.

China has designed new approaches to warfare with new doctrine that specifically challenges our own. Supporting this effort is China's "intelligentized warfare" concept, which applies artificial intelligence's machine speed and processing power to military planning, operational command, and decision support. China routinely conducts national-level and large-scale exercises designed to test its progress with this concept.

China's PLA has reorganized its ground forces to compete with the U.S. Army. The PLA hopes to complete the massive transformation of its force, whereby combined arms brigades, and their parent group armies, field modern, mechanized forces by 2030. China established Theater Commands to manage joint operations and continues to develop new doctrine to enable joint operations. It even created a new branch of service—the Strategic Support Force—that focuses on information warfare, space operations, and cyber activities to back its intelligentized warfare approach. In terms of facilities, the PLA has created several man-made islands in the South China Sea where it can deploy its forces and increase its reach, creating potential overmatch within its so-called First Island Chain.

These modernization efforts are aimed directly at the three assumptions that have been the foundation of the U.S. Army's position of dominance: that the U.S. Army is the best equipped force, best trained force, and the force best at maneuver warfare. Undoubtedly, China will continue to seek methods to erode our traditional strengths, disrupt our national cohesion, and stymy our ability to compete and win.

Article 2: Antiterrorism and Stability Operations

The Chinese Communist Party (CCP) leadership considers terrorism to be a continuing political and military threat, although they routinely blur the lines between true antiterrorism operations and a broader campaign aimed at expanding CCP control over the Muslim ethnic Uyghurs in Xinjiang Province and over separatists in Tibet. The CCP has framed its antiterrorism policy and laws within a broader concept known as the *Three Evils*—terrorism, religious extremism, and separatism—and its conduct of antiterrorism operations has raised grave concerns of widespread and systemic humanitarian abuses against the Uyghurs.[1] Nevertheless, The CCP's antiterrorism response has provided opportunities for bilateral and multilateral cooperation with the United States, particularly against designated terrorist organizations such as the East Turkistan Islamic Movement.

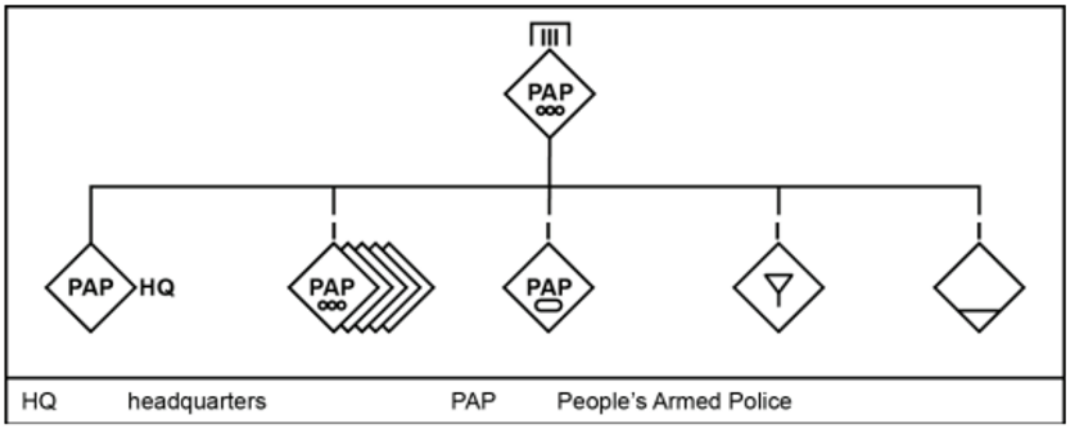


Figure 2. Task-organized People's Armed Police mobile detachment (example)

OVERVIEW OF PLAA ANTITERRORISM OPERATIONS

China takes a far more sweeping position against terrorism than most Western nations. According to official CCP documents, the PLA defines terrorism as acts of violence that disrupt national unity and societal stability and cause casualties or damage to property. The Chinese definition also demonstrates the central role that societal stability plays in the minds of CCP leaders. Instead of only acts of violence perpetrated to achieve a political or social objective, the Chinese definition also includes

[1] Li, Enshen. "Fighting the Three Evils: A Structural Analysis of Counter-Terrorism Legal Architecture in China." *Emory Int'l L. Rev*. 33 (2018): 311.

acts that threaten peace and stability within the country. This, in turn, gives Chinese authorities a broad set of circumstances in which antiterrorism laws and operations can be applied.

Analysis of available PLA doctrine and academic writings indicates that the PLA recognizes several characteristics that shape antiterrorism activities: urgency, complexity, significant effects, joint nature, and asymmetry.

- **URGENCY.** Antiterrorism missions are urgent in nature. Generally speaking, the initiative during a terrorist attack or campaign rests with the terrorist. Proactive antiterrorism efforts are possible, but they are limited in effectiveness by the difficulties associated with identifying and neutralizing potential terrorists before they strike. This makes most antiterrorism activities reactionary and time sensitive. Constant vigilance is important for any unit or organization charged with responding to terrorism and rapid response to a terrorist event is one of the most important elements in preventing casualties, maintaining stability, and preventing further terrorist acts.
- **COMPLEXITY.** Antiterrorism missions are complex. Terrorist activities are sophisticated, often making use of media, religious or political factionalism, civilians, and international actors to manipulate the situation to the terrorists' advantage. Terrorists try to gain regional or global sympathy by framing their attacks as defending religious freedom or promoting justice or democracy. This requires antiterrorism forces to be equally sophisticated and aware of the implications their actions.
- **SIGNIFICANT EFFECTS.** One of the primary features of terrorism is that the psychological and political effects of terrorist acts can often exceed the actual physical effects. Terrorism is designed to amplify the impact of violence by disrupting lives, bringing anxiety to a society, and pressing those conducting antiterrorism efforts to overreact. These effects may be realized even when a terrorist operation fails. A terrorist threat may be enough to achieve the desired effect. Antiterrorism efforts must be valued according to their ability to directly root out and defeat terrorist elements as well as maintain long-term peace, prosperity, and stability of the society.
- **JOINT NATURE.** Antiterrorism operations must be joint in nature. Antiterrorism missions require cooperation between different elements, perhaps more than for any other security activity. The complexity of terrorist activities, along with the fact that they often cross international borders, puts a premium on open and effective cooperation. In this context, joint refers to three different forms of cooperation: between the military, police, and civilian antiterrorism units domestically; between the political and military arms of the government; and between international actors.
- **ASYMMETRY.** Terrorists seldom enjoy parity in equipment or training to that of their opponents, so they instead seek to offset these disadvantages by attacking vulnerable targets. Most antiterrorist organizations are also asymmetric in nature. Terrorists employ ambushes, raids, and sabotage, while antiterrorists employ their own ambushes, along with careful counterattacks, search and annihilate, and infiltration methods.

PRINCIPLES OF ANTITERRORISM OPERATIONS

China believes that the most effective way to reduce any terrorist threat is to suppress it while it is still in its embryonic stage. According to official CCP documents, the Party treats antiterrorism differently than traditional military operations. The PLA and the rest of the Chinese security apparatus are believed to apply the following principles to antiterrorism operations:

- **ACTIVE PREVENTION.** Active prevention requires antiterrorism forces to take constant, targeted, preventative measures to identify and subdue a terrorist plot before it reaches a more active stage. PLA and other Chinese security leaders must also take measures to reduce the vulnerability of terrorist actions by hardening potential targets, keeping the local population informed, and ensuring emergency response capabilities are robust and well maintained.
- **RAPID REACTION.** In spite of the best efforts to actively prevent them, terrorism events typically occur with little or no warning. This requires the Chinese security forces and responders to plan carefully for different contingencies and react rapidly when a terrorist attack occurs. These organizations should be localized and know the population, terrain, and other characteristics of their assigned area. They must train and prepare for different courses of action to save time when actual events occur. When an attack does occur, the planning is quickly updated to meet the needs of the real-world situation. The priorities in these situations are to secure the immediate area, reduce or contain civilian casualties, and rapidly try to kill or capture the terrorists involved.
- **JOINT ACTIONS.** The complex legal framework of antiterrorism activities requires a joint approach to antiterrorism operations. PLAA, PAP, Chinese militia, national police, and local police must are expected to work together under a unified command structure. Because terrorism activities can take on a wide variety of different forms, structures, and capabilities, antiterrorism forces must be able to adopt from passive and cooperative to high intensity postures. Though not observed, it is expected that this approach requires a true joint command that has the authority to unify and coordinate actions across numerous organizations.
- **LEGALITY.** A significant element of a terrorist action is undermining the rule of law and the customs and observances of a population. Some terrorists deliberately attack important institutions to magnify the effect of their violent actions by eliciting reactions of anger and fear from their victims. The PLA recognize that while it may seem prudent in the short term to shelve laws and decency in order to defeat the terrorist threat, behaving in a violent, illegal, or insensitive way toward the local population helps to breed future terrorists and may cost commanders the trust of the people they are trying to protect.

PRINCIPLES OF STABILITY AND SECURITY OPERATIONS

Stability and security operations are conducted in accordance with a fixed set of principles like all other PLA activities. The principles governing stability and security operations are meant to be broader in scope and less restrictive than other Chinese military principles. This is in keeping with the view that stability and security missions are more complex and ambiguous than other operations, and thus they require greater latitude for leaders to act in accordance with their judgment.

- **SITUATIONAL AWARENESS.** While situational awareness is required for military units of all types, it is of particular importance for security units operating in concert with PLA units on an active campaign. Security force commanders must be acutely aware of the general objectives and strategy of the military forces they are supporting, and may be required to operate with little or no direct oversight in securing rear areas, supply and communications lines, and key assets. Security forces may also be required, in dire situations, to face more powerful opponents to delay the enemy or buy time for the supported force to reposition or retreat. Security forces must be prepared to make this sacrifice either when called upon or when they recognize the situation requires it.
- **KEY-POINT CONCENTRATION.** Security forces operate with far less density than do regular army units. Contiguous deployments throughout the security zone are likely impossible, considering available forces and the number of different assets that must be defended. Commanders must carefully prioritize what they want to defend and from what type of threat. This enables the security force to properly allocate its subordinate forces to concentrate greater security on key points throughout the security zone. At the same time, security forces must be able to continue operations even when enemy forces are moving through the security zone.
- **DEFENSE FOCUS.** Security forces may be outnumbered when facing conventional opponents or irregular opponents. This makes offensive actions difficult, as security forces will seldom be able to concentrate sufficient combat power to attack and destroy an opponent. Instead, they must focus on the defense, building their operations around protection of key points, enabled by entrenchments using a defense-in-depth approach. The doctrine of active defense still applies; when a security unit can achieve local superiority, it must attack and spoil the enemy's preparations. Security units contribute significantly to the victory of the larger military force by delaying enemy forces, attrition of enemy formations, or disaggregating enemy capabilities in the security zone, setting the enemy up for decisive defeat by a counterattack.

Chinese military doctrine for antiterrorism and stability operations will continue to evolve to meet the expanding global requirements of the CCP. Currently the PLA's antiterrorism efforts are domestically focused; however, as China's role within the international order expands, the likelihood of Chinese antiterrorism and stability operations in foreign countries will increase. China's increasing expeditionary efforts in stability operations can already be seen in areas of Africa, such as Sudan, where an incident in July 2016 resulted in the deaths of the first Chinese soldiers in hostile action outside China since the end of the Korean War. This means that U.S. forces may encounter the PLA in unexpected areas and must prepare for the associated challenges.

Article 3: PLA Systems Warfare

Systems warfare is the People's Liberation Army (PLA) overarching theoretical framework for identifying and targeting critical or vulnerable systems or the interdependence of systems. The PLA's concept of systems warfare is an adaptation of older Chinese tactical and operational principles. This approach applies to its basic military philosophies; the principles of active defense, deterrence, and deception; and operations in all domains. The PLA classifies all of its capabilities and that of its opponents, ranging from ballistic missiles and strike fighters to cyber operators and special operations forces, as systems. Each system has inherent strengths and weaknesses. The PLA believes that if key adversary systems are rendered ineffective, the enemy's ability and will to fight will crumble.

The PLA's systems warfare concept consists of two fundamental ideas: first, creating purpose-built operational systems that combine key capabilities under a single command; and second, using these operational systems to asymmetrically target and exploit vulnerable components of an opponent's system. If done effectively, this method will render the opponent's key systems ineffective. The PLA believes that by destroying, isolating, neutralizing, or offsetting key capabilities, the enemy's will to resist will degrade, and victory will be achieved.

Systems warfare is the most recent PLA effort to operationalize principles outlined by Sun Tzu and Mao. The PLA's employment of systems warfare supports several traditional military strategies—including preclusion, isolation, and sanctuary—throughout all domains and at all levels of war. Preclusion is achieved by keeping enemy commanders and forces off-balance through asymmetric means, such as deception and information warfare, while simultaneously denying the use of vast geographic areas through long-range reconnaissance-strike capabilities. Isolation is achieved by jamming or manipulating communications between units, employing psychological warfare to confuse and segregate enemy units from one another, then rapidly maneuvering to isolate them physically. Sanctuary is achieved through a mix of protection, defensive planning, information warfare, and deception operations. Sanctuary includes not only safety from physical attack but safety from enemy information operations.

Chinese systems warfare concepts align with some U.S. warfare principles. Chinese systems warfare is similar to the U.S. concept of center of gravity (COG) analysis. Joint Publication 5-0 defines COG analysis as identifying and attacking the critical capabilities and critical vulnerabilities that will affect an enemy's "source of power that provides moral or physical strength, freedom of action, or will to act." Both the U.S. COG analysis and the Chinese systems warfare approach seek ways to destabilize the enemy's ability to mass combat power by bypassing enemy strength and exploiting key enemy weaknesses. However, systems warfare differs from Western military thinking in that it does not consider the human in the fight as an essential element of the combat system. Rather, humans are viewed as subcomponents of systems, to be assessed and targeted like any other subcomponent. China sees adversary's networks as the backbone of the system of systems. Moreover, the PLA appears to recognize domains in the same way as the United States and is actively seeking to enhance multi-domain capabilities and cross-domain integration for systems warfare.

Many of the PLA's systems to prosecute systems warfare are not standing capabilities but rather purpose-built in times of conflict. The PLA intends to build task-organized suites of capabilities to strike specific weak points of its opponent's critical systems during war. These suites of capabilities are called operational systems. Each operational system consists of five main subcomponents: the command system, the strike system, the information warfare system, the intelligence system, and the support system. Building operational systems is similar to creating task forces but broader in scope, trying to develop a comprehensive suite of capabilities under a single command. An operational system consists of several groups—subordinate entities custom-built for a specific mission, task, or purpose. One or more groups represent virtually every battlefield function.

The most common examples of employing systems warfare are targeting networks instead of shooters, sensors instead of aircraft, or command and communication nodes instead of maneuver forces. The PLA includes diplomatic efforts undermining international alliances, offensive cyber operations disabling air or seaport operations, and special operations forces undermining civilian morale through covert operations in systems warfare.

SYSTEMS WARFARE AT THE TACTICAL LEVEL

Warfare typically involves imposing one's will on an opponent by using direct lethal attacks or the threat of attack. The PLA view maneuver as the action to obtain an advantageous position for such an attack. Thus, ground combat units maneuver to isolate their opponents, then defeat them in detail; create numerical or firepower advantages at key locations on the battlefield; or deceive opponents into believing their position to be indefensible. The PLA Army still views land warfare through this lens. However, on the modern battlefield, it sees non-physical attacks as equal to, or more important than, direct lethal attacks. For example, an opponent may be isolated by disabling or denying communications rather than being physically surrounded and cut off. An opponent may believe its position untenable by having vulnerable nodes of its systems rendered ineffective rather than having the systems destroyed. An opponent may view continued resistance as futile—not because of the direct threat of physical force—but because it has been deceived into thinking its situation is hopeless. In other words, system warfare takes the basic principles outlined by Sun Tzu and Mao and applies them to conflict utilizing modern, high-technology weapons systems.

The PLA Army stresses a modular approach to building operational systems for tactical employment. The PLA also recognizes that the less radical the reorganization, the more cohesive a unit will be. The combined arms battalion structure is designed to reflect this. It is the basic building block of the tactical operational system, and it is intended to be employed in something close to its organic or peacetime configuration. Conversely, the combined arms brigade is intended to be easily augmented or task-organized as conditions dictate, flexibly employing a variety of subordinate combined arms battalions, supporting battalions, or other nonorganic capabilities.

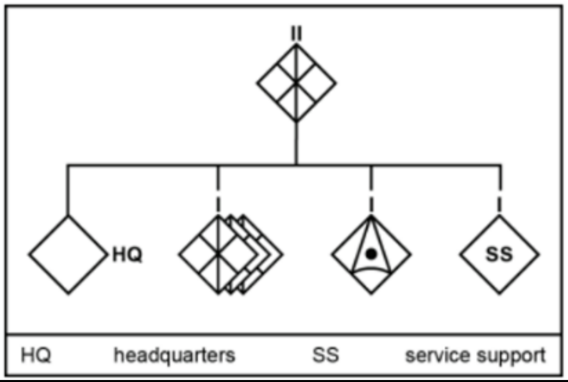


Figure 3. Light Combined Arms Battalion (doctrinal)

At the tactical level, systems warfare focuses primarily on targeting high-value battlefield systems such as radars, command and communication nodes, and field artillery and air defense systems. It can include specific armored vehicles and essential logistics support systems. Examples of tactical systems warfare include using heavy rocket artillery to defeat or destroy enemy radars and artillery systems, electronic warfare to suppress or neutralize enemy command and communication networks, and deception operations to target enemy leadership's situational understanding.

Understanding the Chinese approach to systems warfare is vital to U.S. military preparations for potential conflicts with China. The PLA may describe systems warfare using different official names, including system destruction warfare and system confrontation. Yet, these terms refer to the same basic concept: a conflict wherein systems clash with one another in an attempt to neutralize, destroy, or offset key capabilities and thus grant one side a decisive advantage. Therefore, it is necessary that the U.S. Army identify and protect its critical assets, systems, nodes, and networks. In protecting these components, the Joint Force may be able to mass combat power and achieve the decisive advantage in the event of a war with China.

Article 4: Chinese Information Operations

Information Operations (IO) are one of the most important components of China’s way of war. The People’s Liberation Army (PLA) uses IO to dominate its opponents and separate its adversaries internally and from their allies beginning during the Competition phase with an adversary. The PLA will also use IO continuously across strategic, operational, and tactical missions during the Crisis and Conflict phases. Tactically, the PLA will use IO to detect and acquire long-range targets, execute precise attacks from beyond the line of sight, and conceal its intent.[2] The PLA believes that IO can limit adversarial advantages and reduce threats to its forces.

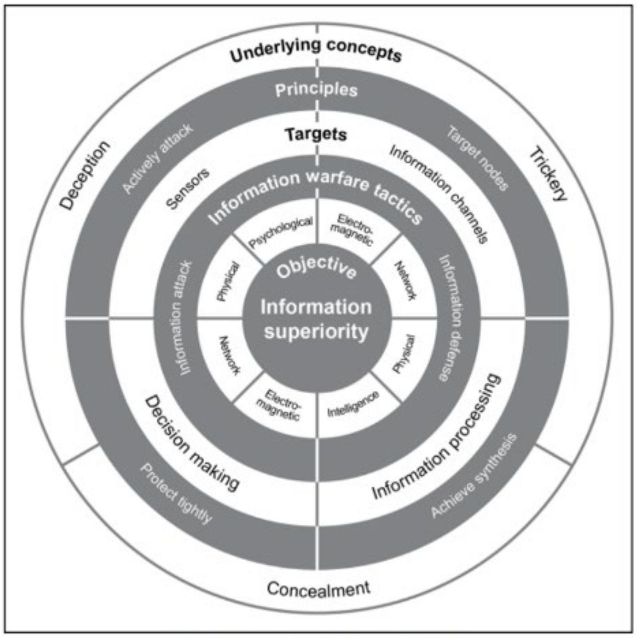


Figure 4. Chinese information operations

IO comprise a wide variety of capabilities with the intent to influence others in the information environment. The PLA’s IO include information warfare (IW)—also known as information confrontation—and psychological warfare. IW, consists of offensive and defensive actions that directly support military operations; whereas, psychological warfare pertains to deception, trickery, and concealment. IW is conducted as part of a campaign, which the Chinese define as a series of integrated operational battlefield activities that target enemy sensors, information channels, information processing, and decision making.

The PLA’s IO objective is to gain information dominance (or superiority). Information dominance means to deprive the enemy of information, deny or disrupt the enemy's ability to control information, and to ensure friendly forces enjoy the freedom of maneuver in the information domain. The PLA considers information dominance to be the new “high ground” in warfare, similar to the view of the air domain during the mid-20th century. Moreover, the PLA sees IO as cost-effective since it can achieve significant effects with relatively minimal expenditure in resources or risk to PLA forces.

The PLA’s IO has four primary characteristics: universal permeation, high target value, the importance of integration and synthesis, and the linkage between attack and defense. The U.S. Army will need to consider these characteristics when it conducts its own offensive information operations so we can achieve our objectives.

- **UNIVERSAL PERMEATION:** IO permeate all domains and are used throughout all campaigns. Due to the widespread reliance on networked systems and information technology, IO affect every

[2] OE WATCH, MARCH 2020*, “Considering The Ground Battlefield Under Informatized Conditions”,* 26-27

aspect of modern conflict. Without information superiority, the Chinese believe that they cannot achieve dominance in other domains: land, sea, air, or space. If the information battle is lost, the PLA cannot gain the initiative for the larger campaign, and campaign activities will be less effective or otherwise blunted. IW will likely begin before formal hostilities, making it an indicator for an armed conflict. IO activities must be planned before hostilities, actively support PLA forces during a war, and be maintained through security and stability operations after hostilities have ended.

- **HIGH TARGET VALUE:** Information systems are high-value targets for Chinese IO. The PLA defines information systems very broadly, including sensors, information management systems, communication network systems, and decision-making centers at all echelons. The Chinese consider information systems to be the brain and senses of a modern force. The PLA prescribes a mix of capabilities, lethal and nonlethal, when targeting enemy information systems. According to the PLA's systems warfare theory, targeting system components is the best way to undermine the rest of the system, and destroying or neutralizing systems is an effective way of neutralizing or defeating a stronger enemy. Therefore, attacking enemy information systems is a high-priority mission, while defending friendly information systems is of equal importance.
- **IMPORTANCE OF INTEGRATION AND SYNTHESIS:** IO require a high level of integration and synthesis of a wide variety of systems, personnel, and functions. Effective integration of these components is one of the unique aspects of IO. Similarly, the broader information campaign must integrate deception, feints, or camouflage tactics to maximize effectiveness.
- **LINKAGE BETWEEN ATTACK AND DEFENSE:** Information attack and defense must be closely linked because the Chinese view them as mutually supporting. Information attack is most effective when friendly information and information systems are carefully protected, while information defense is enhanced when offensive actions disrupt enemy information systems. The PLA believes that the initiative cannot be seized or held without effective integration of both attack and defense. Similarly, the PLA views IO as a zero-sum game, meaning any advantage gained must not be undermined by information lost.

PLA soldiers prepare an attack exercise at a base in Shenyang, China, Aug. 16, 2017. / Source: DOD photo by U.S. Navy Petty Officer 1st Class Dominique A. Pineiro

Four principles describe the PLA's concept of IO: actively attack, target nodes, achieve synthesis, and protect tightly. These principles of tactical information operations must be understood by the U.S. Army and its partners and allies to protect our forces and effectively employ our capabilities in other domains.

- **ACTIVELY ATTACK:** Attack is the primary method to gain the initiative in an IO campaign. The PLA stresses aggressive and integrated attack methods as the best way to attain information superiority. It also believes it is harder to regain the initiative once it is lost in an information war, so emphasis is placed on seizing it early in the campaign. IO's is important in early action because its clandestine nature makes it easily concealed, its low manpower and resource requirements make operational sustainment relatively easy, and reliance on the electromagnetic spectrum makes information systems inherently vulnerable. A robust initial attack takes advantage of these factors, but it requires the conditions to be set long before active hostilities commence.
- **TARGET NODES:** The PLA defines a node as a critical component of an information system that either provides a capability or links other nodes. This context refers primarily to sensors, information processing centers, and the network backbone that enables them. A nodal attack tries to identify, isolate, and target these objects, and it is the centerpiece of the IO campaign. Destroying or neutralizing nodes is the most efficient IW operation: if a critical node is destroyed or neutralized, all systems reliant on it become degraded or disabled. Nodal attack embodies the basic principle of targeting points of weakness, and, if applied appropriately, it can weaken enemy system strong points through isolation and confusion. It is best employed in an

integrated manner with psychological warfare to maximize chaos and extend the effects of nodal destruction.

- **ACHIEVE SYNTHESIS:** For the PLA, synthesis in an IO campaign implies a variety of measures intended to coordinate and synchronize both psychological warfare and IW efforts. Synthesis includes coordinating information attack and defense to maximize the efficiency of both; deconflicting actions so that one does not interfere with another; ensuring that all efforts are unified in their objectives; and, focusing on building mutually supportive efforts that create a larger effect than their separate activities would alone. The concept of adjustment is important to effective synthesis because of the need to assess and change operations quickly without extensive planning. IO are inherently fluid; changes are rapid and often unpredictable. Agility in operations is vital to ensuring IW efforts are pursuing the right targets and achieving desired effects. The primary focus of adjustment is to evaluate different friendly systems and their respective targets and then deconflict actions accordingly.
- **PROTECT TIGHTLY:** Although the PLA views attack as the most important aspect in an IW campaign, it also recognizes that it must blunt the enemy's attacks to gain information superiority. The PLA views information defense as fundamentally more difficult than information attack due to its broad reliance on—and, compared to most adversaries, disparity in—information systems. Indeed, the PLA considers comprehensive information defense to be a practical impossibility, so it emphasizes building systems with resiliency and redundancy. While its information defense is typically passive, the PLA may also use active defense, such as an information attack or counterattack to undermine enemy information attack efforts.

Information Operations are an integral part of PLA operations to shape the operational environment, shaping popular perceptions in contested space, limiting adversaries' relative advantage across the diplomatic, information, military, and economic spheres, and degrading adversarial capabilities. As the United States and our allies continue to work to bolster regional and global partnerships to deter Chinese aggression and malign influence, IO will become an increasingly important tool of Chinese power to contest U.S. efforts to maintain the status quo of the rules based international order. Recognizing what to expect from the PLA's IO—both its characteristics and principles—will help the U.S. Army protect its information processing and intelligence collection capabilities before and during maneuver operations during the Crisis and Conflict phases. Ultimately, effective IO can enable Army commanders to make timely decisions while limiting PLA forces' ability to mass their combat capabilities if Conflict occurs.

Article 5: Chinese Approaches to Unmanned Aircraft Systems

Unmanned aircraft systems (UAS) have changed the face of modern warfare. As UAS have matured in capability, they have taken on a wide range of warfighting tasks. UAS have allowed armed forces to broadly increase intelligence, surveillance, and reconnaissance capabilities, freeing troops and manned assets to handle other activities. UAS have also improved the range and precision of over-the-horizon targeting capability. As UAS technology continues to proliferate, these capabilities will likely reach less capable state and non-state actors. With increased availability, affordability, and capability, threat actors will reduce the United States' traditional technological advantage.

This article covers the current and emerging UAS doctrine of China's People's Liberation Army (PLA), as outlined in ATP 7-100.3, analysis by the Foreign Military Studies Office, and unclassified information from the Worldwide Equipment Guide. Throughout this article, both the terms "UAS" and "unmanned aerial vehicle (UAV)" are used. Unless otherwise stated, "UAS" refers to the entirety of an unmanned system—ground station, operators, and communications networks. "UAV" refers to the specific vehicle, a component of that system.

China is a world leader in UAS development and production, which is reflected in the widespread use of Chinese UAS throughout all echelons of the PLA. The PLA Army (PLAA) employs advanced medium-altitude unmanned aircraft (UA) as surveillance platforms at the theater and group army echelons, and they have likely weaponized some of these systems. PLAA brigades and battalions operate lightweight UA, and units as small as squads or patrols use man-portable UAS. The PLAA also employs weaponized anti-radiation and electronic warfare UA. The PLA Navy uses UAS for long-range surveillance and weaponized variants for antisubmarine operations. The PLA Air Force operates a variety of long-range UAS that support national and theater-level operations and weaponized systems that conduct precision strike missions.

Chinese doctrinal concepts for using UAS on the battlefield are closely tied to the progression from mechanized warfare to "informationized" warfare. Informationized warfare is China's concept for taking advantage of technological change and emphasizes the role of information in **gaining military advantages.[3] The UAS role in informationized warfare is referred to as UAS "Fleet Operations." UAS Fleet Operations centralize management of multiple UAS under a unified command. In an informationized battlefield, UA use onboard computers and common communication networks so that a group of UAS can cooperate. A UAS group can multiply combat power through efficient coordination, enhanced flexibility, and scalability. However, information technology capabilities among the PLA's UAS are not yet fully mature, capable UAS are not fielded across the PLA, and many of its UAS are vulnerable to electronic warfare.**

Reconnaissance is perhaps the most important tasks for UAS in Chinese tactics. According to Chapter six of ATP 700-1.3, deep reconnaissance is broadly defined as reconnaissance operations in areas beyond by a given unit's organic weapons systems. For the PLAA combined arms brigade, this means the areas past the ranges of its tube and rocket artillery, from approximately 35 kilometers (km) to 100 km and extending through the remainder of the theater of operations. This area typically

[3] https://madsciblog.tradoc.army.mil/225-the-pla-close-combat-in-the-information-age-and-the-blade-of-victory/

contains enemy command posts, supply areas, air and seaports, reinforcement routes and staging areas, and long-range fires.

PLA deep reconnaissance operations consist of a mix of long-range, high-endurance UAS; a variety of manned and unmanned ground sensors; long-range SOF and similar light infantry units; and space-based systems. A significant portion of deep reconnaissance assets are organic to the theater command's reconnaissance and intelligence brigade, while others are national-level assets. Deep reconnaissance operations support national and strategic missions as well as tactical operations. Deep reconnaissance capabilities in support of the tactical operations provide targeting for long-range fires, supply commanders with imagery and signals intelligence, and may deliver kinetic effects on enemy formations. Much of the collection performed in support of tactical echelons is performed by manned and unmanned aircraft, with dismounted ground forces in support. UAS may augment observer teams—the most basic element of reconnaissance—and these teams may even operate small UAS without additional support.

The PLAA has also adopted UAS to support its artillery—particularly its long-range rocket artillery. Fire direction, targeting, and forward observation with UAS have been major areas of investment for the PLAA. Combined arms brigade artillery battalions have fire-finding radars, battlefield surveillance radars, long-range electro-optical and infrared sensors, sound-ranging equipment, and well-equipped mounted and dismounted forward observers to integrate with their UAS.. We assess the PLAA's integration of sensors and shooters is agile, redundant, and reliable based on the significant emphasis it places on training for the battlefield surveillance and targeting missions.

Chinese investment in UAS development has resulted in several highly capable UAS that provide a broad spectrum of capability to the PLA. The below examples in the Worldwide Equipment Guide are but a few of the Chinese UAS available.

The Chengdu Pterodactyl, also known as Wing Loong, is a medium-altitude long-endurance UAV, developed by the Chengdu Aircraft Industry Group in China. It is designed for intelligence, surveillance and reconnaissance missions. The air vehicle can also be equipped with air-to-surface weapons for strike operations and perform civil missions such as disaster assessment, meteorological and environmental protection. The system has been compared, at least in appearance, to the U.S. MQ-1 Predator. Based on official marketing material, the Pterodactyl can carry the BA-7 air-to-ground missile, YZ-212 laser-guided bomb, YZ-102A anti-personnel bomb, and 50-kg LS-6 miniature guided bomb.

Chengdu Pterodactyl OE World Wide Equipment Guide

The ASN-105 is a medium tactical UAV in service with the PLA. It is designed to perform real-time battlefield surveillance and intelligence collection. Guided by GPS navigation, the ASN-105B is launched by rocket boost and lands with a parachute. An ASN-105 system is made up of six UAVs, a main ground-control station, a mobile ground-control station, an image-processing shelter, a TV/infrared image interpreting shelter, and a launcher. The ASN-105B may have a redesigned fuselage and changes to the engine. Models displayed in 2004 had a more square-shaped fuselage, increased wing chord and modified engine exhaust. It has a maximum takeoff weight of 160 kg (350 lb) and a ceiling of 6,000 m (19,700 ft).

ASN-105 OE World Wide Equipment Guide

CH-4 OE World Wide Equipment Guide

The Caihong-4, or CH-4, is a long-endurance UAV believed to be in service with the PLA since 2014. It features a 40-hour battery life. The CH-4 is a mixed attack and reconnaissance system with six weapons and a payload of up to 345 kg. It can fire air-to-ground missiles from an altitude of 5,000 meters (16,400 feet); therefore, the aircraft can stay outside of the effective range of most anti-aircraft guns. Externally it is similar to the Pterosaur air vehicle with a V-shaped tail, long wingspan, and tail propeller but with a redesigned nose.

China's development and proliferation of increasingly advanced UAS will pose a risk to the U.S. Army including from loitering munitions and new doctrinal concepts to employ these systems. This risk will evolve as China moves from informationized warfare to intelligentized warfare, developing new doctrinal concepts to employ these systems, such as employing loitering munitions and swarming small autonomous systems that are networked and cooperating to achieve a military objective. Chinese military theorists believe that autonomous swarming systems "…will likely become the "blade of victory" in the hands of commanders at all levels on the future battlefield."[4] In that vein, the U.S. Army must learn to counter current UAS threats while keeping an eye toward the future.

[4] Mad Scientist Blog 225, April 2020, TRADOC G2, Translated from Jiefangjun Bao, 2020, 225. The PLA: Close Combat in the Information Age and the "Blade of Victory" | Mad Scientist Laboratory (army.mil)

Article 6: Planning and Organizing Army Operations and Command Post Operations

The planning process of the People's Liberation Army (PLA) has deep roots in Chinese military theory. However, the this planning process continues to evolve with ongoing force structure modernization, including in the PLA Army (PLAA). As the PLAA moves toward a more modular force structure, it will likely increase emphasis on developing a more decentralized command process.

Movement toward greater decentralization, modular combined arms units, widespread downsizing, and the creation of new headquarters at the national and theater command levels have reshaped the PLAA's planning and command processes. The PLAA was once a strongly centralized and hierarchical force, relying on a mix of discipline and obedience to overcome shortcomings in technology and firepower. However, the modern PLAA has advanced its technological capabilities and firepower, which to be used most effectively requires greater decentralization. The modern PLAA recognizes that it requires a more sophisticated understanding of command and support relationships; improved professional military education for its commanders, staffs, and noncommissioned officers; and continued doctrinal adjustments as new equipment and technologies enter the force. Consequently, the PLAA planning and command processes are continuing to evolve.

PLAA's COMMAND POST OPERATIONS

The PLAA defines a command post as a temporary command structure formed around a commander and staff. The number and type of command posts the PLAA uses are situationally dependent, with up to four typically used to control operations: a base command post, an advance command post, a rear command post, and a reserve command post. Command posts are led by a commander and manned by various command groups. Certain command posts—most likely those more forward on the battlefield—may be designed as mobile command posts, making it more challenging for the enemy to detect and target them.

- **Base Command Post:** The base command post (also called the main command post) is the primary command structure, and it is the center for executing command throughout the operational area. The PLAA try to ensure the base command post is well protected, well concealed, and near the center of the operational area. The commander operates out of the base command post, along with the chief of staff and primary staff officers. The base command post controls several activities including: command and communication, reconnaissance and intelligence, firepower coordination, electronic warfare and cyber warfare, engineering, battlefield management, and political work.

- **Advance Command Post:** The advance command post (also called the forward command post) is a forward-based structure designed to enhance command and communication in a key direction of the battle. Ideally, it is situated near the main offensive or defensive effort, and it is well concealed and protected. The advance command post is typically led by the deputy commander and staff. It has a command and communication group, a reconnaissance and intelligence group, and a firepower coordination group.

- **Rear Command Post:** The rear command post (or alternate command post) is responsible for logistics and equipment support, along with rear area security. It consists of a combat support and service support group headquarters, a political work group, and security personnel. The commander of the combat support or service support group is often the commander of the rear command post. The rear command post serves as the primary backup command post in case the base command post is destroyed, neutralized, or otherwise compromised. In some situations, the deputy commander may choose to operate from the rear command post.

- **Reserve Command Post:** The reserve command post is a backup in case one of the other three command posts is compromised, damaged, destroyed, or otherwise neutralized. It is smaller and less capable than the base command post, but it must be able to conduct all base command post operations. The reserve command post may also serve as an interim command post in case the other command posts are temporarily unavailable due to movement or enemy action.

PLAA's PLANNING PROCESS

The PLAA has been known throughout its history for its meticulous approach to planning operations, and this tradition remains in place today. Though the PLAA seeks to gradually move to an increasingly decentralized leadership structure, careful planning at all echelons remains a basic principle.

The PLAA planning process is broadly similar to the U.S. Army's Military Decision-making Process. The primary outputs of the planning process are the operation's objectives, the scheme of maneuver, and the structure of the operational system to conduct the operation. The operational system may include multiple subordinate operational systems and specialized supporting systems.

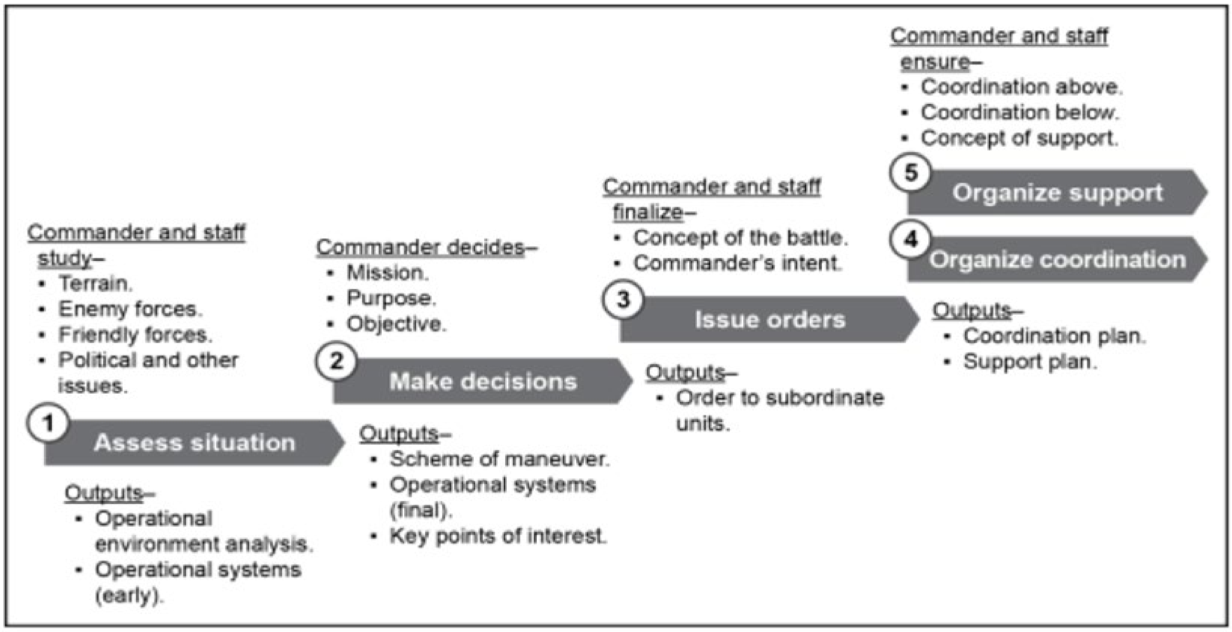


Figure 5. PLAA Planning Process

The PLAA's planning process consists of five steps, each with distinct outputs. Subordinate units conduct planning concurrently with their higher echelon headquarters and adjust their plans according to inputs received from it. The planning process seeks to achieve unity of purpose throughout the operation by ensuring that all subordinate commanders know their role, mission, and place in the wider operation.

- **Step 1 – Assess the Situation:** During this step, the commander assesses four critical components of the operation: terrain, enemy forces, friendly forces, and other considerations, such as civilian presence and political elements. The outputs from this step include an early outline of the desired friendly operational systems, a comprehensive report on enemy strength and disposition enabled by reconnaissance and intelligence support, and a thorough analysis of all other factors in and around the battlefield that may influence operations for either side.

- **Step 2 – Make Decisions:** This step requires commanders to make several key decisions that determine the direction of the rest of the planning process and the overall operation. Commanders must establish the purpose and objective of the operation, the general scheme of maneuver, the basic structure of the operational systems under their command, and key offensive and defensive points of interest. The output of this step allows subordinate commanders to begin their own planning process, staffs to begin building operational systems, and command posts to establish command systems. Focused reconnaissance operations should also commence at this point to support the intelligence requirements for the overall operation.

- **Step 3 – Issue Orders:** This step consists of two main phases. First, commanders convey the concept of the battle to their staffs, accounting for enemy strengths and disposition, friendly forces, and the higher echelon commanders' intent. The staff then creates an order that clearly lays out the commander's concept so that subordinate units can easily understand it. Second, the order is issued to subordinate units, either verbally or in writing. Ideally, orders are issued to subordinate commanders in groups, allowing subordinates to ask questions and collaborate with one another prior to conducting their own planning.

- **Step 4 – Organize Coordination:** This step refines the orders issued in step 3. Staffs conduct planning that synchronizes purpose between subordinate units, ensures that adjacent units' schemes of maneuver are integrated, and provides predictions about how the battle will be conducted. It also clarifies issues of confusion with subordinate commanders and ensures that shared resources and enablers—such as communications and network support—are coordinated.

- **Step 5 – Organize Support:** This step organizes external capabilities that support the operation. Examples include combat support, logistics support, equipment support, and political support. Specific capabilities include firepower and artillery support, information warfare, sustainment, casualty evacuation, and medical support. This step requires staffs to interact with external enablers; higher echelon staffs may provide assistance in building this part of the plan. Commanders must account for available resources, mission requirements, and friendly forces when developing the support plan.

The PLAA’s command post structure and planning cycle resemble the U.S. Army Tactical and Main command post structures and troop leading procedures. However, one key difference is the PLAA’s integration of political officers into its command-and-control processes. U.S. Army leaders should understand the similarities and differences of the PLAA planning process to understand how the PLAA prioritizes aspects of its operations and where control of an operation occurs.

Article 7: Planning the Offense

The China's People's Liberation Army (PLA) has historically stressed the importance of careful planning and preparation before an offensive operation. This focus continues in the post-reform PLA Army (PLAA), where offensive actions are developed, rehearsed, revised, and carefully executed whenever possible. Meticulous planning allows for integrating capabilities, developing tight security measures, and building an effective deception plan. While devoting more time for planning may reduce speed in the short term, the PLAA believes that a well-constructed and well-rehearsed plan ultimately saves time and increases operational speed.

PLAA offensive operations are objective-based: the higher echelon commander designates an objective and specifies a force charged with accomplishing it. Mao's "People's War" principles dictate that objectives should typically be enemy formations, although key terrain or other valuable assets may also be considered. The attacking force identifies key features in the defense and terrain, including disposition of enemy forces, points of strength and weakness, and locations of reserves and fire support. The offensive action is then designed to rapidly confuse and isolate the enemy, reducing its morale and enabling freedom of action for PLAA commanders. Through a combination of careful planning, effective deception, rapid movement, and application of decisive combat power at key times and locations, the enemy comes to believe its position to be untenable and it must either withdraw or face annihilation. Once the enemy force is in retreat, PLAA reserve forces maintain contact and pursue the enemy while additional forces secure the area and prepare for follow-on operations.

BUILD THE COMMAND SYSTEM

A PLAA offensive operation entails at least two, but ideally all four, of the command posts discussed in the previous article. The base command post is the commander's primary location during an offensive, and it should be located to best coordinate between the frontline, depth, and thrust maneuver groups. The advance command post, if established during an offensive, is led by the deputy commander and is typically located near the main defensive line. The rear command post's primary role is to organize logistics and reinforcements and to create the backup defensive line supporting the offensive action. If possible, a reserve command post is established along a possible route of egress or in a well-defended rear location, ready to take over for the base or advance command post should either of them come under threat during an offensive. At the combined arms battalion echelon, the command and limited staff may be decentralized rather than physically co-located.

The offensive battlefield is further subdivided into between two and four operational zones, each with a specific set of objectives and tactics. These zones are deep area, frontline zone, reserve zone, and garrison zone. While the PLAA used to be highly prescriptive about the physical sizes of these zones, it has gradually moved to a more flexible approach. The various zones should account for terrain, friendly and enemy capabilities, and higher echelon missions, and they should enable careful integration of various units and capabilities.

Deep Area. The deep area is the territory past which a unit's organic sensors and weapons can operate. For a combined arms brigade, this typically means the area past which its rocket artillery and targeting support can operate. The fight in the deep area usually consists of independent special operations forces (SOF) or scout units supported by manned or unmanned aircraft (UA), possibly augmented by supporting fires from long-range shooters assigned to support the offensive action. Reconnaissance, counter-reconnaissance, fire, counterfire, screening, and blocking all take place in deep areas. The purpose of deep-area operations is to provide early reconnaissance, target long-range preparatory fires, and carefully assess enemy strength and disposition in preparation for an offensive action.

Frontline Zone. The frontline zone contains the territory in which the main offensive action is to occur. Early objectives, along with the enemy's main defensive line, are typically located in the frontline zone. The frontline attack group is the primary occupant of this zone, and the depth group may also occupy the area, depending on terrain and enemy disposition. The advance command post, if present, is usually forward in the zone, and the base command post is typically located either rearward in this zone or in the zone immediately behind it. The entire frontline zone should be within the range of the offensive group's organic fire support. The frontline zone typically contains a security zone on its forward edge, where security, reconnaissance, and counter-reconnaissance activities take place. The primary battle takes place in the frontline zone, with the intent of breaching the enemy's main defensive line and enabling the depth and thrust maneuver groups to move into enemy rear areas.

Reserve Zone. The reserve zone lies just to the rear of the frontline zone and typically houses the depth attack group, thrust maneuvering group, reserve group, command groups, firepower groups, and forward logistics bases. The reserve zone also usually contains a defensive line intended to resist enemy counterattacks into rear areas, and serves as the anchor for the offensive action. The reserve command post, if present, is typically located in this zone, as is the rear command post.

Garrison Zone. Rear areas not actively occupied by the offensive group make up the garrison zone. Augmentations and reinforcements may reside in this zone, or it may serve as an assembly area for another offensive group preparing to conduct follow-on operations. Supporting capabilities such as logistics, electronic warfare (EW) assets, and long-range artillery reside here. Garrison zones typically contain one or more security zones that surround key positions, such as bases, supply routes, or command posts. The People's Armed Police (PAP) may take on much of the security load in garrison zones in order to free up PLAA forces for more intense duties.

PHASES OF THE OFFENSE

The PLAA's offensive operations are divided into phases in much the same way that U.S. Army operations are organized. While an operation may have many phases depending on the breadth and complexity of the mission, in most cases it will involve five primary phases: advance, unfold, initiate, annihilate, and continuing operations.

Advance. The advance, also called the moving-in, is the initial phase of an offensive operation. This traditionally referred to the movement of a main body from a staging or assembly area to the initial point of attack. For a modern force, this understanding has expanded to include the full breadth of activities that occur between when the mission is received and initial contact is made. These activities include, but are not limited to—

- Security throughout the combat area, including assembly areas, staging areas, axes of advance, and flank areas.

- Reconnaissance operations focusing primarily on the objective: assessing the enemy force and probing for possible weak points or vulnerabilities.
- Counter-reconnaissance operations attempting to deny the enemy key information about PLAA forces' dispositions and objectives.
- Deception operations designed to mislead and confuse the enemy, conceal friendly movements, fix enemy formations, and manipulate the enemy's mindset.
- Artillery groups delivering preparatory fires, reconnaissance by fire, and counterfire.
- Air defense groups seeking to deter air attack against the main body and to deny aerial reconnaissance to the enemy.
- Engineer groups conducting both mobility and countermobility operations along enemy and friendly axes of advance.
- Protection operations seeking to maintain the force, especially during periods of vulnerability to air or artillery attack.
- EW activities seeking to degrade or neutralize enemy sensors and communications, while protecting friendly network systems and emitters.

The advance begins upon receipt of an order. Reconnaissance groups are rapidly deployed to determine possible routes of advance, enemy strength and disposition, and key terrain features. The commander develops an initial scheme of maneuver that outlines objectives, establishes a basic concept, and enables subordinate units to establish contact and rapidly close with enemy defenses. Concealment of movement and deception operations are critical during the advance phase. It is at this time that the commander can most influence enemy actions, dispositions, and mindset. As the main body moves to the point of contact, supporting capabilities conduct concurrent missions, including preparatory fire support, counterfire, information warfare activities, and mobility and countermobility activities. Commanders continuously assess enemy positions to decide on a final course of action while trying to manipulate the enemy's mindset and conceal their own intentions. As reconnaissance groups develop the situation, the commander decides on a final course of action.

Security during the advance is also of the utmost importance. Deception operations can only be successful if enemy reconnaissance operations are neutralized, spoofed, or defeated by friendly counter-reconnaissance. Security elements ensure that main body movement is unhindered by enemy attack, countermobility efforts, or deception activities. Air defense and protection operations ensure that the main body is not attritted by enemy air attack and artillery during staging or movement.

The advance phase ends when the main body makes contact with the enemy and the commander initiates actions on contact.

Unfold. The unfold phase consists of actions designed to set conditions for annihilation that occur upon initial contact by the main body with enemy defenses. Subordinate units conduct rapid movement in accordance with the commander's scheme of maneuver, seeking to position themselves appropriately for the decisive phases of the operation. Following initial contact, units maintain contact with the enemy and continue to develop situational understanding. Key intelligence requirements not yet answered by reconnaissance groups are resolved by main body actions. During initial contact, the commander tries to conceal the direction, strength, and objective of the main effort through deception, information warfare activities, feints, and demonstrations. Other activities during the unfold phase include, but are not limited to—

- Security operations, particularly to the flanks and rear, to protect the main body from spoiling attacks or counterattacks.
- Reconnaissance operations moving deeper into enemy areas.
- Counter-reconnaissance operations that defeat enemy attempts to identify the main effort and objectives while reinforcing deception efforts through feints and demonstrations.
- Deception operations meant to fool the enemy commander about the time and place of the main effort; the size, strength, and disposition of friendly forces; and the size and proximity of reinforcements for both sides.
- Artillery groups shifting fire support focus to counterfire, obstacle reduction, and disruption efforts in deep areas.
- Air defense groups deterring or defeating aerial attack and surveillance throughout the area, with an emphasis on the main body and main effort.
- Engineer groups shifting focus to obstacle reduction and maintaining friendly mobility.
- EW focusing on jamming or spoofing enemy communications to impede rapid response to the attack.

The primary goal of the unfold phase is to ensure that the objective is isolated and contending with numerous dangers, preferably from multiple directions. The enemy commander should be confused and enemy forces disrupted. The enemy, however, should not yet know either the direction or strength of the main effort. The entire unfold phase should be orderly and well planned in order to ensure concealment and correct positioning of friendly units. Movement should be rapid, but not so fast that confusion sets in or concealment is broken.

The best practice of the unfold phase is to encircle the enemy or to convince the enemy it is encircled. Encirclement refers to the complete isolation of the enemy force through a combination of friendly ground unit actions, firepower, deception, psychological warfare, and EW. Encirclement does not necessarily mean that an enemy is actually physically surrounded. A combination of lethal and nonlethal capabilities may be sufficient to cause the enemy to believe itself encircled. For example, a well-timed artillery raid may cause the enemy to believe that a route is cut off or unavailable, without requiring the commitment of additional PLAA ground forces. Similarly, disinformation passed over communications channels may deceive the enemy into believing it does not have access to a particular route or terrain, without requiring friendly forces to physically occupy the area in question.

The unfold phase ends when the main effort commences.

Initiate. The initiate phase begins when the main effort commences its assault against the objective. This phase often begins with a massive assault wherein fire support groups target enemy command nodes, critical systems, mobile reinforcements, and other high-value targets. Supporting efforts continue to develop the situation. Units charged with fixing enemy units continue to prevent them from reinforcing the main objective, while counter-reinforcement groups preclude the commitment of enemy reserves. The main effort is typically the primary assault upon the enemy's center of gravity: that thing—be it a headquarters, a unit, or a piece of terrain—that is most essential to the enemy's morale and mindset. Ideally, the enemy will either withdraw, collapse, or be routed once the center of gravity is seized or destroyed. Other activities during the initiate phase include, but are not limited to—

- Security operations continuing with the primary objective of protecting the main body from spoiling attacks or counterattacks.
- Reconnaissance operations focusing on intelligence objectives that support the main effort.
- Counter-reconnaissance operations continuing to spoil enemy efforts to discover the composition, axis, and objectives of the main effort.
- Deception operations continuing to fool the enemy commander about the time and place of the main effort; the size, strength, and disposition of friendly forces; and the size and proximity of reinforcements for both sides.
- Artillery groups conducting a firepower assault, delivering massed fire support to the main effort, targeting defending enemy units, interdicting movement of reinforcements, and destroying or suppressing command and communication nodes.

Attacks are launched from multiple directions simultaneously, forcing the enemy commander to make decisions about force deployment. If possible, the enemy commander's decision cycle is interrupted—or, better yet, influenced—so that reinforcements or other maneuvers do not concentrate in opposition to the main effort. The main effort employs substantial force concentration to achieve local firepower and numeric superiority over the enemy, enabling defeat of the enemy's forces in detail and maintaining the initiative. Fire support is weighted heavily in support of the main effort's assault.

The main effort targets one or more primary objectives as a part of the assault on the enemy's center of gravity. These may include enemy command posts, assembly areas, reserve forces, artillery units, or network nodes. The main effort seeks weak points in the enemy's defense, then moves rapidly to penetrate them. Follow-on forces help to secure the main effort, fix or deceive remaining enemy forces, and preclude enemy reinforcement. Groups—possibly airborne, air assault, SOF, or militia—located to the flanks and rear of the enemy secure key terrain to prevent outside reinforcement of the enemy formation while encircling the objective. Supporting groups ensure that enemy counterattacks—particularly counterencirclement—are spoiled, disrupted, neutralized, or defeated before they can affect the main effort.

The initiate phase is complete once the main effort seizes the enemy center of gravity.

Annihilate. The annihilate phase commences after the enemy is confused and demoralized following the seizure or fall of its center of gravity. Enemy units should be isolated, with communications to their higher echelons disrupted and routes for reinforcement either cut off or unusable. The enemy is encircled, either physically or psychologically, and mutual support between enemy units is no longer possible. Decisive attacks are conducted throughout the combat area, seeking to destroy isolated enemy units before retreat and a prepared defense are possible. Fire support is used aggressively in brief but violent volleys to suppress and demoralize enemy units prior to assaults. Special focus is given to ensuring that the enemy cannot break out of the annihilation zone. Security and countermobility efforts slow or stop movement before enemy units can escape.

Once the enemy recognizes that one of its units is facing annihilation, a strong response is likely inevitable. Enemy air and artillery units will try to target friendly formations to suppress or disrupt friendly attacks. Antiair and artillery groups must be prepared to conduct counterair and counterfire operations in response. Other enemy ground formations will try to reinforce their besieged units. Friendly security forces must defend stubbornly and disrupt, slow, or defeat these attempts until the objective force has been annihilated.

The annihilate phase ends once the objective force has been destroyed, routed, or has surrendered.

Continuing Operations. Continuing operations commence immediately when it is clear that the objective force has been destroyed, routed, or has surrendered. The remainder of the enemy force loses cohesion in the face of decisive attacks throughout the combat area, and widespread withdrawal or retreat follows. The main focus during this phase of the operation is pursuit of these fleeing enemies. High-tempo operations continue to maintain contact with these enemy forces during their retrograde, defeating rear-guard security actions and preventing the enemy from consolidating to form a coherent defense. Counter-reinforcement groups continue to defeat enemy attempts to reinforce the area by either defeating enemy forces, spoiling enemy attacks, or conducting countermobility operations.

When continuing operations commence, the commander begins assessing follow-on opportunities. For example, if defeating the enemy unit created a breach in the enemy's main defensive line, an opportunity for envelopment or penetration may be present. Similarly, the enemy unit's defeat may create an opportunity for the PLA to highlight the success of the operation to influence public opinion. Units may begin transition from combat postures to movement postures in accordance with the scheme of maneuver. However, if a unit redeploys into march order too soon, it may be vulnerable to enemy counterattack. If it waits too long, opportunities for penetration or envelopment may be lost.

The PLAA unit must also consolidate. Consolidation comprises three primary activities: performing security activities, reorganizing and reconstituting friendly units, and conducting passage of lines. Security activities consist of securing the combat area against enemy reconnaissance and counterattack and ensuring that friendly forces entering the area are not subject to threat from bypassed enemy elements or irregular forces. Reorganization and reconstitution are those activities that enable the unit to conduct resupply, replacement of lost or damaged equipment, casualty processing, and receipt of reinforcements. Passage of lines takes place when one unit passes through another's combat area, typically with the intent to resume offensive operations against the enemy. Passage of lines can be a complex task, and it is enabled by effective control measures, communications, and planning.

This meticulous planning involved in the PLAA's operations, coupled with the trend toward modularity and decentralized command, will allow the PLAA greater flexibility in conflict. As technology advances, modularity and decentralization could increase the effectiveness of Chinese units in a theater as geographically dispersed as the INDOPACOM area of responsibility.

Article 8: PLA Offensive Action Principles in the Informationized Environment

Throughout its history, the People's Liberation Army (PLA) has emphasized offensive operations. The idea that war can only be won by attacking is fundamental to Mao's People's War theory, and China tested it throughout the Chinese Civil War and the Korean War. PLA leaders historically have emphasized the spirit of the attack—what Westerners would call élan or esprit de corps—as the only way their military forces could overcome the technological, firepower, and training superiority of their opponents. Developing this spirit in their formations was a fundamental skill of PLA leaders. Indeed, the role of political officers and commissars was in large part to help develop a unity of purpose underpinning the spirit of the offensive.

The PLA Army (PLAA) today takes a similar view toward offensive operations. In keeping with Mao's principles, PLAA operations focus on destroying enemy formations rather than taking ground. PLAA forces seek to use a mix of maneuver, deception, and firepower to preclude enemy actions, isolate enemy units, and then fight the isolated enemy to annihilation. PLAA units integrate advanced deception and information warfare capabilities to fix enemy forces and then conduct decisive attacks on enemy weak points. They employ firepower not only as an enabler of maneuver, but also as an offensive tactic in itself: employing massed fires to destroy, neutralize, or fix opponents. As such, objectives are often described as enemy formations.

PLAA offensive operations are performed to accomplish one or more of the following objectives:

- Destroy, defeat, or neutralize enemy formations, personnel, or equipment.
- Enable friendly freedom of maneuver.
- Restrict enemy freedom of maneuver.
- Gain information.
- Gain control of key terrain.
- Disrupt enemy operations.

This article draws from Chapter 7 of ATP 7-100.3 outlining the PLAA's methodology for planning and executing tactical offensive actions. The PLAA considers tactical offensive actions to be the decisive form of land operations. China's active defense strategy relies on effective and credible tactical offensive actions, which destroy an opponent's will to fight, as the basic contribution of ground forces.

OFFENSIVE OPERATIONS IN AN INFORMATIONIZED BATTLEFIELD

The PLAA recognizes six important trends related to transparency, precision munitions, electronic warfare (EW), operational tempo, multidimensional battle, and cost that impact offensive operations on the informationized battlefield. PLAA leaders and planners must account for these trends when considering and conducting all types of offensive operations.

THE TRANSPARENCY OF THE INFORMATIONIZED BATTLEFIELD. Advanced multispectrum surveillance, networked intelligence, and the connected world have combined to make true deception much harder to achieve than it was in the past. Units will find it far more difficult to assemble, move, and prepare for offensive operations without the enemy uncovering their intent. Commanders are instructed to integrate deception plans across the entirety of the information spectrum, and they must always assume that they are being surveilled by a clever enemy.

THE PROLIFERATION OF PRECISION MUNITIONS. Precision munitions enable rapid, deep, and precise targeting of critical assets across the informationized battlefield. Firepower no longer requires mass; effective synchronization of precision munitions can achieve the same effect that formerly required dozens of attack sorties or hundreds of guns. Precision platforms usually overlap one another to achieve a combined arms effect, and their targeting is enabled by advanced multispectrum surveillance. Commanders must always assume the enemy can strike them. Commanders must reduce vulnerability by physically and electronically protecting their forces, neutralizing or defeating attacks by precision munitions, moving rapidly, and deceiving the enemy to throw off its targeting process.

THE IMPORTANCE OF EW. The PLAA not only puts a high priority on its own offensive EW capabilities, it also anticipates that enemy EW capabilities will contest its network and communications capabilities. EW has the potential to offset precision munitions, sensors, and joint communications networks, creating an environment where aggression and short-range firepower can prove decisive. As this is equally true for both Chinese forces and their opponents, electromagnetic protection is a high-priority PLAA mission. PLAA leaders and units are instructed to train in communications blackout conditions, relying on ingenuity and tactical competency to overcome the effects of communications isolation, and wherever possible, use communications means that are not susceptible to enemy EW efforts.

THE RAPID TEMPO OF OPERATIONS. The informationized battlefield moves quickly, and changes in the environment can be unpredictable and sudden. Motorized and mechanized ground units, along with aerial units, can traverse vast distances in short periods of time. Firepower systems can range distant targets and react quickly to new targeting information. All of these developments likely mean that windows of opportunity for commanders to seize the initiative are getting smaller. Commanders must be mentally agile to take advantage of these windows in the absence of direction from higher echelons, particularly if the situation deviates from the planned one. Comprehensive planning and training helps to ensure that units can take advantage of the smallest window of opportunity when it is presented.

THE MULTIDIMENSIONAL BATTLEFIELD. The informationized battlefield involves all dimensions and domains. Thus, commanders must think three dimensionally and integrate capabilities across all domains. The PLAA fears enemy airpower, multispectrum surveillance, and precision firepower, and it seeks to offset these capabilities through integrating its different operational systems. At the same time, commanders and planners must ensure that PLAA forces can strike through all domains in a synchronized, intelligent manner, to effectively isolate enemy units and defeat advanced enemy systems.

THE FINANCIAL COST OF MODERN WAR. The weapons that populate the informationized battlefield are high technology and often very expensive. Outfitting an entire force is an exercise in national economics as much as military strategy. Precision munitions are lethal and effective, but they are also expensive and stockpiles of them are minimal. The logistics train, which begins with manufacture and ends on the battlefield, must be up to the task of supplying the PLAA with sufficient modern systems and munitions.

Once initial stockpiles are depleted, whichever nation or military that can best sustain its forces will enjoy a significant advantage in combat.

The PLAA is advancing its capabilities and doctrine to win offensively against the U.S. Army. As a result, U.S. Army leaders should take note of the preparation and considerations the PLAA makes for the modern battlefield. PLAA firepower, joint integration, and maneuver concepts provide U.S. Army leaders with valuable insights into Chinese military thought. As the PLAA continues to evolve from mechanized to informationized and further to intelligentized operations, offensive actions and capabilities will remain of the utmost importance.

Article 9: PLAA Defensive Operations

Though the People's Liberation Army (PLA) considers the offense to be the decisive form of warfare, it emphasizes defensive operations because centuries of invasion and occupation have made defending Chinese territory from outside aggression the PLA's most sacred mission. Additionally, the PLA Army (PLAA) believes that defense is an inherently stronger form of war, as the defender enjoys advantages of terrain and time unavailable to the attacker. The informationized battlefield, however, has reduced these traditional advantages.

A well-planned and coordinated defense is a critical component of every combat action. The objectives of the defense are to attrit attacking enemy forces, retain key positions or terrain, buy the commander time and decision space, seize the initiative from the enemy, and transition to offensive operations. While it is not possible to destroy an opponent through defensive actions alone, a tenacious and well-executed defense enables decisive follow-on offensive operations.

As we have seen with the offense, the shift in Chinese military thought from mechanized to informationized warfare has also changed the PLAA's paradigm of defensive operations. The following article is an excerpt from Chapter 8 of ATP 7-100.3.

DEFENSIVE OPERATIONS IN THE INFORMATIONIZED BATTLEFIELD

The PLAA still maintains that defense is a fundamentally stronger form of warfare than offense, but it acknowledges that many elements of the informationized battlefield have changed the traditional dynamics between attack and defense. Most—though not all—of these changes benefit the attacker, making defensive operations more difficult than they have been historically. The PLAA has identified four major trends on the informationized battlefield that influence defensive operations: increasing arduousness, fewer inherent advantages, more dynamism that is required, and the increasing importance of offensive actions.

Increasing Arduousness. Multiple factors have combined to make combat for the defender more difficult than in the past. While ground commanders once only had to concern themselves with enemy land forces, enemies can now strike simultaneously or consecutively from multiple domains. This requires, in turn, a comprehensive multidomain defense that can effectively blunt or check enemy actions, even when coming from unexpected directions. Commanders must also defend their forces not only from physical attack, but also from information, electromagnetic, and psychological attack: a capable opponent will target enemy troops' morale and cohesion through a variety of channels. Finally, the depth and variety of enemy firepower systems have increased substantially in recent years. Long-range artillery and missile strikes, air strikes, attack helicopter operations, direct action by special operations forces (SOF), and electromagnetic and network attack capabilities allow an enemy to target the full depth of friendly formations and defended areas. There is no safe space on the informationized battlefield.

Fewer Inherent Advantages. Historically, a defender enjoyed several fundamental advantages that translated to nearly every combat action: greater ability to conceal one's forces and deceive the enemy; better use of terrain to cover and harden one's position; improved communications and coordination due to interior lines and known terrain; and more time to make the best use of the deployment area and battlefield depth. Conditions on the informationized battlefield have eroded all of these advantages. Concealing one's own forces and deceiving the enemy about deployments and dispositions is far more difficult because of advanced wide-area multispectrum intelligence, surveillance, and reconnaissance capabilities. In the past, one only needed to win the ground reconnaissance and counterreconnaissance battle, but the informationized battlefield uses air, space, and cyber intelligence collection in addition to more advanced ground-based capabilities. Precision munitions and long-range strike capabilities have eroded several basic defensive advantages offered by terrain, making it far more difficult to effectively harden defensive positions. The enemy can also effectively target the command and communication systems of a defensive position in ways never before available. Electronic warfare methods, such as communications jamming and meaconing, and network attack are capable of destroying, disabling, degrading, or manipulating the command and communication backbone of a defensive position. Finally, the defender's classic advantage of depth has been eroded or eliminated by capabilities that enable the enemy to strike into deep areas. Deep areas that were once generally considered secure can now be targeted with both lethal and nonlethal attack methods, even when many miles from forward areas.

More Dynamism that Is Required. As modern offensive operations demand rapid thrusts that target weak points from unexpected directions, the common practice of defending strong points with a relatively static approach is now obsolete. Static formations, even in a strong defensive position, will quickly be bypassed, isolated, and then annihilated by a competent attacker. Instead, defense must be considered a dynamic action characterized by rapid movement and decisive concentration of combat power at key times and places. Information superiority coupled with mobility, enables the defender to rapidly detect and appropriately respond to enemy offensive actions, regardless of where they might occur. This approach to defense is in keeping with the PLAA's new emphasis on decentralization because lower-echelon commanders must be able to react appropriately to unexpected events without input from a higher echelon. While the hasty defense was once considered a last-ditch option, it is today the cornerstone of a PLAA defensive operation versus a capable opponent.

Increasing Importance of Offensive Actions. While seeming somewhat paradoxical, offensive actions within a broader defensive operation are considered to be of heightened importance. Due to the conditions of the informationized battlefield, counterattacks have increased in their lethality and unpredictability. A well-timed and -executed counterattack can disrupt, defeat, or spoil an enemy's offensive action just as effectively as a well-planned defense, and the counterattack enjoys all the advantages of other offensive actions: enhanced firepower, enhanced reconnaissance, multidomain options, and the elements of surprise and initiative. The PLAA approach to defense-by-offense prescribes the use of depth attacks and aggressive maneuver to put the counterattack group in the best possible position, concentrating combat power against enemy weak points and enabling the isolation and destruction of enemy offensive groups.

HOW THE PLAA PLANS THE DEFENSE

PLAA doctrine prescribes a large number of steps for planning and executing a defensive operation, which can be consolidated into seven major phases:

- Build the command system.
- Organize reconnaissance.
- Organize the defensive group and deploy.
- Spoil the enemy’s preparations.
- Resist the enemy’s assaults.
- Counterattack.
- Consolidate or withdraw.

Each phase is part of every defensive operation to some degree, but the phases are not necessarily sequential. Because they are largely in response to enemy actions, they may be conducted in varied order or concurrently. The planning for these phases includes organizing the defensive battlefield and building the defensive groups that comprise the operational system.

Build the Command System. As with offensive operations, the PLAA prefers to carefully plan and organize major defensive operations. Meticulous planning enables greater redundancy and depth in the defense, improved overall security measures, a more effective deception plan, and a greater chance of a decisive counterattack. The centerpiece of the defensive plan is the deployment of the command posts. A defensive operation makes use of at least two, and ideally four, command posts. The base command post is the commander’s primary location, and it will typically be located to best coordinate between frontier defense and depth defense units, oriented toward the enemy’s anticipated main axis of attack. The commander may also establish an advance command post in a more forward position. The rear command post is led by the deputy commander, and it is deployed in a well-defended location. Its primary role is to organize logistics and rear area defense. If possible, a reserve command post is established along a possible route of egress or in a well-defended rear location, ready to take over for the base or advance command post should either of them come under threat.

The PLAA makes careful use of terrain and geographic control for the defense. There are two primary features that a commander must identify to make best use of the terrain. First is the main direction of defense, which informs the combat group of the orientation of the enemy’s anticipated primary effort. Commanders are expected to take into account higher echelon and adjacent-unit missions, specified defensive tasks, the unique characteristics and tendencies of the opponent, and terrain throughout the defensive zone. Second, the commander must establish key defense points (KDPs). KDPs are the specific features within the defensive zone that are most important to the integrity of the overall defense. They are not limited to key terrain and may include a command or network node, a key unit or leader, or even a piece of information. Commanders should keep the number of KDPs small, choosing only those points critical to the successful execution of the defensive battle. KDPs should also be phased, allowing for them to change during the course of the battle. The defensive plan should be centered on maintaining these KDPs, which assists commanders in prioritizing their available resources.

The defensive zone is subdivided into between two and five secondary zones, each with a specific set of objectives and different set of tactics: deep area, frontal blocking zone, frontier defense zone, depth defense zone, and rear defense zone. While the PLAA used to be highly prescriptive about the physical sizes of these defensive zones, it has gradually moved to a more flexible approach. These secondary zones should account for terrain, friendly and enemy capabilities, and higher echelon missions. They should also facilitate integration of friendly units and capabilities.

Deep areas are those that are not targetable by a defensive group's organic weapons systems. They may still be occupied by elements of the defensive group conducting reconnaissance, counter-reconnaissance, and screening missions, but these elements operate independently. SOF elements also occupy deep areas, and both air and missile support may be employed in support of deep-area operations. The primary purpose of deep-area operations is to disrupt and slow the enemy advance while providing the defensive group commander with critical intelligence about the enemy's strength, disposition, and possible objectives.

The frontal blocking zone is the forward-most area of the defensive zone. It is analogous to the Western security zone, and it is designed in much the same way. The frontal blocking zone is occupied by units performing screen or cover missions, and it serves as the primary early warning, disruption, reconnaissance, and counter-reconnaissance zone for the main body. The frontal blocking zone should orient toward the enemy's primary axis of advance—particularly its primary reconnaissance axis. This zone should be positioned sufficiently in front of the main body to give the commander time and decision space, usually between 3 and 5 km for a combined arms brigade. The frontal blocking zone is likely occupied primarily by the cover group.

The frontier defense zone is typically the combat group's primary defensive area. It should contain most KDPs and the preponderance of combat power. Units should seek to conduct a strong defense within the frontier defense zone, trying to force the enemy to commit most of its combat power and leave its forces vulnerable to counterattack. The frontier defense zone is primarily occupied by one or more frontier defense groups and possibly a depth group. Operations in this zone are centered largely on active resistance to enemy assaults. Fortifications and entrenchments should be as extensive as time and resources allow, and units should be prepared to conduct stubborn and brave resistance, possibly in the face of significant odds. The base command post is typically located in this zone, while the advance command post will be either forward in the zone or rearward in the frontal blocking zone.

The depth defense zone extends behind the frontier defense zone, and it serves as the deep area of the defensive zone. Depth defense groups—the heart of the counterattack force—are deployed here to react quickly and appropriately to the enemy's assaults in the forward defensive areas. Combat reserve groups may be stationed in this zone to reinforce or assist forward units. A single depth defense zone may serve as the deep area for multiple frontier defense zones. Operations in the depth defense zone should ensure mobility, protection of the depth defense group from air or artillery assault, and the concealment and secrecy of counterattack operations. The reserve command post, if established, will likely be located in this zone.

The rear defense zone is the deepest area of the defensive zone, and it contains logistics, equipment support, and other rear area units and capabilities, including the rear command post. This zone is occupied primarily by rear area security units—possibly People's Armed Police (PAP) units in addition to PLAA security forces—and it may also house depth or the combat reserve groups. The rear defense zone ensures protection against enemy deep artillery, air strikes, and enemy SOF or guerrilla actions in rear areas, and it ensures mobility to enable retrograde or reinforcement movements through the zone.

Organize Reconnaissance. The reconnaissance effort is a critical enabler of a defensive operation. Reconnaissance must be comprehensive and well planned, extending through all domains and the depth of the battlefield. This effort concentrates on three primary intelligence objectives: disposition and intent of enemy forces; terrain; and conditions of the battlefield—civilians, weather, the electromagnetic environment, and so on. Reconnaissance commences immediately upon receipt of warning orders: commanders rapidly build and deploy the reconnaissance and intelligence group to facilitate rapid, accurate, and continuous scouting for the main body. Deep and forward reconnaissance units surveil and disrupt enemy forces in deep areas. As the situation develops, additional reconnaissance forces, having been held in reserve, are deployed to key areas of the battlefield to enhance situational understanding.

Reconnaissance groups are often charged with disrupting enemy operations, typically as part of a screen or cover force. This requires a mixture of stubborn resistance and prudent tactical offensive actions, usually in the form of raids coupled with entrenched units. These activities are intended to force the enemy to deploy earlier than it would like, buying the commander decision space and revealing the enemy's plan of action. At the same time, counter-reconnaissance actions are meant to spoil the enemy's efforts to ascertain friendly force dispositions, leaving it ignorant as to the strong and weak points of the defense. Reconnaissance screens may try to funnel or steer enemy forces toward areas of strength.

Reconnaissance information should be carefully analyzed and processed to give the commander the clearest possible picture of the battlefield. The commander must identify the most important elements of information, and the reconnaissance and intelligence group must strive to answer any questions as clearly and accurately as possible. Intelligence filtering enables the commander to judge friendly and enemy situations; make best use of terrain, weather, and the conditions of the electromagnetic spectrum; and then distill the ground truth from the "fog of war." In contrast to its historical approach of top-down intelligence, the postreform PLAA places greatest value on the lower-echelon commander's situational understanding, above that which is handed down by upper-level leadership. Lower-level commanders are encouraged to act decisively based on their own judgment, though they must consider the higher-echelon mission and intent.

Organize the Defensive Group and Deploy. The combat power that comprises the defense is organized into a defensive group, the combat group assigned to the defensive mission. This operational system is built in the same way as any other tactical operational system, using the combined arms brigade as the primary force provider and the combined arms battalion as the primary building block. Capabilities are organized into one of four primary groups, each with a distinct mission: the frontier defense group, the depth defense group, the combat reserve group, and the cover group. A combat group may contain some or all of these, and it may contain more than one of each. Additional groups that may be employed include a firepower strike or artillery group, an air defense group, an electronic and network warfare group, and a combat support group. In addition, the commander may designate teams for specific missions, such as antitank, mobile artillery, obstacle construction or reduction, or rear defense.

Once the defensive group is assembled, groups deploy to the defensive zone. This action should be undertaken quickly, allowing time for adjustments and amendments to orders after the groups reach their initial positions. The cover group typically has the mission of scouting, occupying, and securing the defensive area, enabling the other groups to move into place quickly and safely. Any enemy reconnaissance or scouting elements in the defensive area must be aggressively attacked and driven off, ensuring secrecy of movement and disposition of friendly forces. These operations are likely performed in tandem with ongoing friendly reconnaissance efforts.

Secrecy of movement is a critical component as follow-on friendly forces occupy their assigned defensive positions. Commanders are expected to assume that the enemy is watching and should employ concealment and deception as much as possible. Commanders are also expected to account for the threat of artillery bombardments, airborne or ground-based radars, and information operations efforts targeting the combat group throughout this phase.

Engineering construction begins immediately as the groups enter the defensive position. Engineers' priorities are determined primarily by terrain, enemy capabilities, and time available. A hasty defense may only allow simple structures, such as improvised obstacles and firing positions. With more time available, a more elaborate defense may allow for extensive tunnels, entrenchments, field structures, permanent shelters, and fallback positions. The PLAA emphasizes the use of irregular units, such as local militia and local populations, for engineering construction efforts. All engineering efforts focus heavily on KDPs.

Spoil the Enemy's Preparations. Once the reconnaissance efforts determine the enemy's presence and disposition, the defensive group commences efforts to spoil the enemy's offensive plan. In most cases, this phase involves two primary efforts: spoiling attacks and firepower assaults. Ideally, these efforts are conducted concurrently to achieve a combined-arms effect. Spoiling efforts are not intended to be decisive; instead, they are seen as enabling the main defensive efforts and eventual counterattacks.

Spoiling attacks, also called harassing attacks or harassing assaults, are limited-scope offensive actions that are designed to disrupt enemy movement and cohesion, reduce enemy morale, develop PLAA situational understanding, and manipulate the enemy commander's decision making. Spoiling attacks may take the form of offensive ground action, air attack, or information attack. Spoiling attacks target key enemy formations or capabilities, trying to engage them when they are in a vulnerable state, such as during movement. Ground spoiling attacks often employ hit-and-run tactics—such as raids—and commanders are warned not to become decisively engaged. Enemy assets such as communications systems, high-value weapons systems, and lines of communication (LOCs) are the most prized targets. Forces that conduct spoiling attacks are often expected to act independently, and thus they must be skilled and flexible. Objectives for spoiling attacks may include disrupting enemy command and communication to forward units, inflicting casualties, destroying or neutralizing key systems, and slowing the enemy's advance. Spoiling attacks occur throughout the defensive operation, and they are of particular importance in defeating any enemy breaches of the main defensive line.

Firepower assaults employ artillery groups or firepower strike groups to target enemy offensive forces with destructive massed fire. The firepower assault may employ a firepower assault zone, a predetermined and pretargeted area serving as an ambush point. If employed, firepower assault zones should be located along the enemy's expected avenue of approach or on terrain the enemy is likely to occupy. A firepower assault seeks to decimate the enemy formation when it is most vulnerable, either during movement or during a halt in open terrain. The best practice is to integrate the firepower assault with other attacks, particularly spoiling attacks by reconnaissance forces, to maximize the accuracy of fire and the combined-arms effect of multidimensional threats. Commanders must, however, ensure that the groups that conduct the firepower assault do not expose themselves to enemy counterfire unnecessarily, as it is likely that the enemy would conduct a counterfire attack once it discovers friendly artillery forces. Commanders may employ mobile artillery in the firepower assault role or may rely on hardening or deception to protect their artillery force.

Resist the Enemy's Assaults. The main defensive effort occurs when the enemy commences its main assault through the defensive zone. The enemy's attack consists of a mixture of maneuver, firepower, and information attack. It is coordinated and synchronized to overwhelm, destroy, or force the withdrawal of friendly units. The focus of the resistance phase is to blunt the enemy's attack; sap its combat power, cohesion, and morale; and put it in a vulnerable position. This allows the defender to seize the initiative through aggressive counterattacks and then transition to the offense. The PLAA anticipates fighting throughout the depth of the defensive zone, and it offers three guidelines to inform commanders during this critical phase: wage simultaneous resistance, prioritize combat strength, and use proper countermeasures.

The enemy's attack will likely target the full depth of the defensive zone with depth assaults, flanking assaults, and encircling maneuvers. These various actions must be resisted using a comprehensive and integrated approach. Resistance may take the form of symmetric, force-on-force actions—such as meeting an armored thrust with an armored reserve—or it may be asymmetric, such as using an electromagnetic attack to confuse and neutralize an enemy air depth assault. Commanders must anticipate heavy enemy activity within the defensive zone and skillfully and flexibly move their own forces—taking advantage of interior LOCs and knowledge of terrain—to meet and defeat the various enemy actions. Commanders primarily employ blocking actions and repositioning actions during resistance.

Blocking actions involve a group or unit standing fast and tenaciously defending a specified position, with the intent to stop or delay an enemy action, reduce enemy cohesion, and inflict casualties on enemy units. Blocking actions should only be conducted when necessary, or when terrain or other factors make such actions highly advantageous, because they make a unit or group vulnerable to encirclement, isolation, and firepower attack. Blocking actions should be supported with firepower, obstacles, and reinforcements. They are ultimately intended to enable follow-on actions, such as counterattacks.

Repositioning actions are movements conducted by units or groups during the course of the defense. Commanders mix repositioning and blocking actions to conduct a tenacious withdrawal, ceding unimportant territory to the enemy only after inflicting heavy casualties. Skillful defense alternates blocking and repositioning in such a way that resistance is continuous and no unit is ever exposed to enemy assault.

Effective resistance is underpinned by effective prioritization of combat strength. This guideline references the broader People's War principle of prioritization, but with a focus on defensive action. As a defensive group is assaulted through multiple domains and from multiple directions, the commander makes decisions about how and where to commit reserves and reposition units. Enemy thrusts should be met with the least amount of force believed necessary. This differs significantly from offensive actions, where commanders are encouraged to concentrate as much combat power as possible against key objectives. Commanders should seek to minimize movement—especially long-distance movement—

during critical phases of resistance. If a unit must move long distances, it is essentially unavailable as a fighting force. Commanders must prioritize the value of moving a unit during a defensive action, carefully considering the loss of the unit's combat power during the movement period and the vulnerability of the unit to enemy action. High-quality, comprehensive reconnaissance and intelligence is essential to effective prioritization.

Even the best defensive action is inherently reactionary. The defensive group must assess and react to the enemy, rather than dictating the fight on its own terms. This means that defensive combat places a higher premium on employing the right tactical means to counter enemy capabilities. Commanders must have a clear picture of the enemy capabilities they are facing and build operational systems to effectively counter their anticipated opponent. So too must commanders rapidly and effectively react to the enemy's actions as the situation unfolds, deploying friendly combat power to counteract enemy penetrations and assaults.

Counterattack. The counterattack, also called the mobile assault, is typically the culmination of a defensive operation. It requires the defensive group to mass combat power and conduct an aggressive, decisive attack against one or more enemy units, with the intent of disintegrating the enemy attack and forcing the enemy to either rapidly retreat or face annihilation. Counterattacks happen throughout a defensive action on smaller scales, but the decisive counterattack at the tactical level likely involves either the depth defense group or the combat reserve group conducting multidimensional penetrations of an enemy assault force. These penetrations target weak or exposed flanks of the enemy formation.

The timing and axis of the counterattack is critical. It should be timed to the moment when the enemy attack has culminated, and enemy forces are possibly overextended, low on supplies, and beyond their supporting or security elements. Resolute defense throughout the frontal blocking zone and the frontier defense zone should create favorable conditions for the attack, magnifying the combat power of the counterattack force. A counterattack should include one or more of four phases, which may be concurrent or in varying order.

The first of these phases, concentration of firepower, is often the touchstone that begins the counterattack in earnest. Commanders may use any combination of indirect fire—possibly in the form of a firepower assault—direct fire, and information attack, concentrated on the most powerful part of the enemy's formation. In many situations this will be the enemy's armored spearhead, and so the concentration of fire should involve a large number of antitank weapons. Concentrated fire disrupts the enemy's attack, creates casualties, and destroys key weapons systems, opening a window of opportunity for the counterattack to break through the enemy's exposed flank.

Neutralizing significant or dangerous breakthroughs is the second phase. Enemy forces that have achieved significant penetrations in the defensive zone can threaten the counterattack with defeat or destruction. Breakthroughs can be sealed off using firepower or direct attack, or the can be neutralized by attacking enemy LOCs. Sealing off breakthroughs does not mean that the enemy units must be annihilated; it only ensures that they cannot threaten the counterattack force as it conducts its mission. Once the counterattack is successful, the remaining enemy units will be isolated and encircled, enabling their destruction or forcing their withdrawal.

The third and decisive phase of the counterattack should take the form of a small-scale offensive operation. Ideally, a commander executes an attack that involves penetrations from multiple directions and through multiple domains, preventing the enemy from massing combat power and confusing it about the disposition and axis of the main effort. Direct assaults on the enemy's front are the preferred method of attack, as this fixes the enemy and immediately targets its most valuable units. Pincer movements are considered a secondary approach, and while they may be effective at targeting the enemy's exposed flank, they require longer movement and more time, which exposes the counterattack force to enemy artillery or direct attack. Firepower assaults can cut off or block access to the rear, while blocking units work to stop further penetrations. The assault targets the enemy's center of gravity, attempting to isolate enemy units throughout the defensive zone.

As the counterattack commences, commanders assess its effectiveness. If it is effective, they may order fourth phase to commence, a continuation of the attack or consolidation of the gains. If it is ineffective, they may order the counterattacking force to assume a defensive posture and resist any further enemy advances. Regardless of effectiveness, commanders must immediately deploy the defensive group to retain KDPs, whether they are still held by friendly forces or have been recently retaken by enemy forces. Commanders should anticipate the enemy sending reinforcements or conducting supporting attacks promptly after it recognizes the threat of the counterattack. Having the defensive group deployed and in place to block these attacks helps to ensure that the gains achieved by the counterattack are not lost.

Consolidate or Withdraw. During or after the counterattack commanders face a critical decision about how to proceed with the defensive battle. If the counterattack succeeded in decimating, blunting, or neutralizing the enemy assault, commanders may consider ordering a follow-on attack into the enemy's depth. Alternatively, they may consider holding fast, reinforcing and entrenching the current position to better resist any further enemy assaults. Commanders must consider casualties sustained, the overall readiness of available troops, the vulnerability of the enemy, and the advantages gained by each course of action when making a decision to continue advancing or hold in place.

If the counterattack was unsuccessful or the defensive group suffered serious casualties during the counterattack, the commander may order a withdrawal. The withdrawal should be orderly and decisive, with available groups conducting alternating retrograde operations and blocking actions. No unit should ever be exposed to an enemy pursuit attack. The deployment of air defense groups to deter or defeat attack by air is particularly important. Units are particularly vulnerable to firepower attacks during withdrawals. Concealment and cover are important for the unit, and the firepower or artillery groups must prioritize counterfire operations if any unit is in the process of withdrawal.

The PLAA prescribes a general order of precedence for a combat group's withdrawal. First, the cover group exits the frontal blocking zone. Next, all support and logistics groups exit the rear area. Then the main body and firepower and artillery groups exit the frontier defense zone. This leaves the combat reserve, or rear group, to conduct a rearguard or screening action in the rear defense zone, ensuring that all other groups move to safety. The combat group commander must designate an assembly area that is both accessible and defensible, then rapidly establish a new defensive zone and begin entrenching as quickly as possible.

Understanding PLAA defensive actions will be necessary for U.S. Army leaders and warfighters at all levels. Chinese defensive doctrine, coupled with the PLA’s strike capabilities, may preclude the Joint Force from being able to mass combat power in the manner that was seen before Operations Desert Storm and Iraqi Freedom. The PLAA views the defense as central to a successful military campaign, but it believes that offensive operations will be decisive to any future victory. The growing sophistication of Chinese technology, the advancement of theory and the character of warfare, and the importance of integrated campaign planning present formidable obstacles in the event of armed conflict between China and the United States and our allies. Each of these factors increase the importance to the U.S. Army of operating effectively as a Joint Force and with key coalition partners if we are to prevail.