Hearing Statement of Lt General David A. Deptula, USAF (Ret)
U.S.-China Economic & Security Review Commission
27 January 2011
"China's Active Defense Strategy and its Regional Impact"

Thank you very much for the opportunity to testify before this hearing on China's active defense strategy and its regional impact. In my testimony I will address each of the questions you posed to me in your letter of invitation as follows:

- Describe the regional security implications of the People's Liberation Army's capability to integrate military operations in the western Pacific across all domains of war.
- Explain the role of space in what the United States calls China's antiaccess strategy. How might China's space operations degrade, disrupt, deny or destroy U.S. military capabilities in the event of a conflict between China and the United States?
- Explain the cyberspace-related aspects of China's area control and antiaccess strategy. How might China's cyber operations degrade, disrupt, deny or destroy U.S. military capabilities in the western Pacific in the event of a conflict between China and the United States?
- Discuss other non-traditional strategies that the PRC could use to affect U.S. operations in the western Pacific, such as what the Chinese military calls "the Three Warfares" (that is, psychological operations, influence operations, and legal arguments).

Regional Security Impacts of Integrated People's Liberation Army (PLA) Operations

Question

Describe the regional security implications of the PLA's capability to integrate military operations in the Western pacific across all domains of war.

Introduction

Prior to the late 1970's, PLA operational doctrine was largely defensive, focused on using China's strategic depth to gradually wear down an opponent. PLA doctrine has since evolved into a principle called *active defense*. Active defense is based on the capability to rapidly project force in response to external threats, seizing the initiative at the outset of the conflict. The PLA has developed a framework for doctrine-driven reform with the long-term goal of building a force capable of conducting "local wars under informatized conditions." The PLA relies on a body of principles and guidance known as the "National Military Strategic Guidelines for the New Period" to plan and manage the development and use of its military. This document most likely dates from 1993 with enhancements in 2002 and 2004. The operational, or "active defense" component the People's Republic of China (PRC) strategy, posits a defensive military strategy in which China does not initiate wars or fight wars of aggression, but engages in war only to defend national sovereignty and territorial integrity. Once hostilities have begun, the essence of active defense is to take the initiative and to annihilate the enemy. Strategically, the

guidelines emphasize active defense, in military campaigns the emphasis is placed on taking the initiative in active *offense.*

Implementing Active Defense

The PLA is developing and implementing supporting doctrine for "active defense" warfare and new operational methods across the services. PLA modernization has been driven by a Taiwan contingency for most of the past 20 years but recently, modernization efforts have begun looking beyond Taiwan towards a regional power projection capability.

PLA Air Force (PLAAF) The PLAAF continues its conversion from a force for limited territorial defense to a more flexible and agile force able to operate off-shore in both offensive and defensive roles. The PLAAF focuses on improving their ability to conduct air strikes, air and missile defense operations, early warning and reconnaissance as well as strategic mobility. The PLAAF also has a leading role in conducting a "Joint Anti-Air Raid" campaign, the operational doctrine for much of China's antiaccess and area-denial operations. The anti-air raid campaign is strategically defensive in nature, but at the operational and tactical levels, it calls for attacks against adversaries' bases and naval forces.

China has one of the most sophisticated and dense integrated air defense systems (IADS) in the world. Long-range SAMs include Russian SA-20/GARGOYLE and indigenously-produced HQ-9s. These systems are deployed in overlapping layers around key population centers and strategic centers, to include full coverage of the Taiwan Straits. China's IADS also include numerous medium and short-range systems. The PLAAF also uses Russian-built Su-27 and Su-30 fighters as well as the indigenously produced F-11B and F-10 multi-role fighters. The recently unveiled fifth-generation J-20 low-observable fighter will give the PLAAF another air superiority fighter. The PLAAF also has strike capability with their Su-30MKK fighters and long-range B-6 Bombers.

PLA Navy (PLAN) The naval component of active defense is termed "Offshore Active Defense." The 2008 PRC Defense White paper describes the PLAN as a strategic service continuing to develop the capability to operate in distant waters. Regionally, the PLAN is focused on the Yellow Sea, East China Sea, the Taiwan Strait, and the South China Sea, following the contours "first island chain." The PLAN is also developing capabilities to operate in the "second island chain," which reaches out to Guam. PLAN doctrine for maritime operations focuses on six offensive and defensive campaigns: blockade, anti-sea lines of communication, maritime-land attack, anti-ship, maritime transportation protection, and naval base defense.

The PLAN is focused on fielding modern destroyers, submarines, cruise missiles, and maritime strike aircraft to deter or prevent an adversary from operating near China's coast. China's submarine force is a key component of their sea denial strategy. KILO submarines have both land attack cruise missiles (LACM) and anti-ship cruise missiles (ASCM). The new indigenously produced SHANG nuclear attack submarine gives the PLAN its first global strike capability, capable of launching conventional LACMs. The PLAN likely will deploy its first aircraft carrier when the refurbished Russian Kuznetsov-class carrier is deployed next year. The PLAN also has maritime strike capability with its Su-30MKK force.

Second Artillery (Missile Force) Ballistic missiles play a key role in China's force projection plans and efforts to deny foreign military forces access to the region. China has the most active development program and largest deployed conventional ballistic missile force in the world with a variety of ranges, payloads and capabilities to strike aircraft carriers, airfields, command and control facilities, logistics

nodes, ports, and military bases. Over 1,000 short, medium and intermediate-range ballistic missiles are deployed opposite Taiwan. Among the warheads believed to be either fielded or in development are runway penetrators, anti-radar seekers, variable delayed-fuse penetrators and other specialized warheads. China has also developed an anti-ship ballistic missile, the CSS-5 mod 4 anti-ship ballistic missile (range up to 1600 nm) , that could threaten US aircraft carriers, potentially forcing them to operate at a longer range from the Chinese coast. Complementing ballistic missiles are long- and medium-range LACM that can be launched from aircraft, ships, submarines and mobile ground-based platforms. China's medium-range missiles such as the CSS-5 (range up to 1350 nm) and the DH-10 LACM (range up to 1100 nm) put all US bases in South Korea and Japan at risk, as well as alternate locations in the Philippines or Malaysia. The Chinese have also developed standoff LACMs which give them the capability to conduct precision strikes from well outside the range of defensive systems. These include the long-range air-launched YJ-100 (~1,000NM) and the medium-range YJ-63 (135NM).

Integrated Joint Operations

The Chinese term for integrated military operations is integrated joint operations (IJO). Recent efforts toward more integrated operations are embodied in the January 2009 edition of the PLA Outline of Military Training and Evaluation (OMTE). The PLA is focused on training, equipping and sustaining their force to conduct multi-service operations in an informatized environment. IJO specifically refers to multiservice campaigns controlled by a joint headquarters with an integrated command and control architecture, but the services still conduct separate operations. IJO are dependent on a well developed C4 environment, integrated and effective intelligence, surveillance and reconnaissance (ISR) coverage, interconnected weapons platforms as well as coordinated logistics. As IJO matures over the next 5-10 years, the PLA will increasingly be able to bring to bear their warfare capabilities in the five domains of war including the land, sea, air, space, and cyberspace spectrums.

To rectify deficiencies in IJO, the PLA has launched enhanced training and professional military education, cross-training rotational assignments to different services, war simulations, and multi-military region (MR) exercises. In 2009, the PLA conducted at least three high-profile joint exercises through mid-September, including a joint ground-air exercise involving cross-military region deployment of up to 50,000 troops, a joint campaign exercise to train theater-level commanders in joint operations, and a joint anti-terrorism exercise with Russia. This effort continued in 2010 with Mission Action, a multi-region air and ground exercise. Ground forces were transported across military region boundaries and were supported by the PLAAF. The exercise focused on the operational level of war with group army headquarters responsible for command and control, overseen by the general staff department.

Regional Implications of IJO

The modernization of the PLA, coupled with an increasing capability to conduct IJO over all domains of war, represents a growing threat to the US and other countries in the region. These augmented capabilities can be used in coercive diplomacy and to contest territorial disputes by force, or threat of force. Increasingly, the PRC is focusing on developing capabilities that project power throughout the region, enhancing China's position in Asia and the world military hierarchy. When the PLA is able to effectively conduct IJO, antiaccess operations against the U.S. in the western Pacific will become more effective. U.S. operations, both air, missile and maritime, from mainland Japan, Okinawa, and the Philippines will be severely impacted. The PLA will likely be able to degrade and/or deny US air- and space-based surveillance and reconnaissance capabilities in the region. Command and control of deployed U.S. forces will likely be disrupted and it will be more difficult to logistically support operations in the western Pacific. It is also likely that U.S. aircraft carriers will be forced to operate at

distances far from the PRC mainland. Lastly, as China continues to fund military modernization in the smaller Asian countries and invest economically in the region, their control over the military and economic actions of these countries, will increase. This is likely to push the operating environment to one that is increasingly unfavorable to the U.S.

Role of Space Operations in China's Antiaccess Strategy

Question

Explain the role of space in what the United States call's China's antiaccess strategy. How might China's space operations degrade, disrupt, deny or destroy U.S. military capabilities in the event of a conflict between China and the United States?

Introduction

China recognizes the overwhelming advantage the US has in the space domain and its key role in our ability to collect, analyze and rapidly share data. They understand how dependent U.S. warfighters have become upon space products and services for commanding deployed troops, passing ISR data, and enabling precision targeting and engagement. China views that reliance as a significant, exploitable vulnerability and has written extensively about the subject in both open source journals and military doctrine. As a result, they are actively pursuing a comprehensive array of space and counterspace programs intended to degrade, disrupt, deny or destroy our ability to gain and maintain access to the region in the event of a conflict.

Space Weapons

China maintains a development and deployment program for space weapons including programs on direct ascent anti-satellite (ASAT) weapons, high energy laser (HEL) and dazzlers and GPS and other types of jammers. The PRC is developing these weapons and technologies as a way to counter U.S. space superiority and to deny the use of space. China understands the U.S. reliance on space for imagery, signals intelligence, communication, tracking of friendly forces and navigation. As such, they are developing the capabilities to deny the U.S. information at the time of their choosing. Additionally, the threat of space denial, such as through the testing of ASAT weapons, is also an effective counterspace strategy.

ASAT Weapons China understands how the U.S. uses our large fleet of military and intelligence satellite systems to find, fix, target and track Chinese military forces, then use our array of communication satellites (COMSATs) to pass that data to our deployed forces and finishing with our GPS navigation satellites (NAVSATs) to target and engage with precision. In January 2007, China successfully tested a direct ascent (DA) ASAT missile against a Chinese weather satellite, demonstrating its ability to attack satellites operating in low-Earth orbit (LEO). This test has been widely viewed as a direct challenge to U.S. space superiority. In addition to ASAT, the PRC is researching methods of co-orbital interception to target our NAVSATs and COMSATs. Co-orbital ASATs will provide China with a broad range of options beyond kinetic attack to counter our space-enabled, information advantage. For example, In June 2010, China launched the Shijian-12 (SJ-12) satellite from Jiuquan Satellite Launch Center in north-central China. According to the State media service Xinhua, SJ-12's mission is to carry out "scientific and technological experiments". However, between Jun 20 and Aug 16, SJ-12 conducted a series of maneuvers to rendezvous with SJ-06F, an older Chinese satellite launched in Oct 08. SJ-12 made many close approaches with less than 984 feet between the two satellites. China could

conceivably want to experiment with close space maneuvers, given its plans to build a space station that would require continuous resupply. However, the lack of official Chinese information about the maneuvers has allowed room for speculation that China has now demonstrated a capability with potential application to co-orbital ASAT capability.

Space Object Surveillance and Identification (SOSI) Implementation of these ASAT options requires not only the weapons themselves, but also information about the physical characteristics and orbits of the satellites to be targeted and attacked. China currently is developing a SOSI network to improve its space situational awareness. This network will give it the ability to track and identify most satellites for offensive actions while allowing for deconfliction with Chinese satellites. Beijing will continue to enhance its satellite tracking and identification network, as it is the first step in establishing a credible ASAT capability.

Directed Energy Weapons (DEW) The PRC also plans to interfere with the flow of information by targeting high-altitude GPS and communications systems using ground-based jammers. In this way they can degrade GPS/communications reception or employ deception against our combat aircraft and precision-guided munitions. Techniques such as radiofrequency jamming, laser attack, high-power microwave or electromagnetic pulse detonation will allow China to deny us these data sources without generating debris that might impact their own military use of space. PLA-affiliated publications assert that while China does not yet possess the capability to destroy satellites with high-powered lasers, they are capable of damaging optical reconnaissance satellites.

Role of Counterspace Operations in China's Antiaccess Strategy

Publicly, China opposes the militarization of space, and seeks to prevent or slow the development of anti-satellite (ASAT) systems. Privately, however, China's leaders probably view ASATs, and offensive counterspace systems as force multipliers. As one Chinese defense analyst noted: "For countries that can never win a war with the United States by using the method of tanks and planes, attacking the US space system may be an irresistible and most tempting choice". Even a limited ASAT capability would be extremely useful to the PLA in contingencies involving the Taiwan Strait.

Prior to hostilities, the Chinese would likely use directed-energy weapons (DEW) such as high energy lasers (HEL) to dazzle or blind our imagery satellites. This technique would be intended to negatively impact our ability to monitor Chinese military activities while maintaining a degree of deniability and reversibility for Beijing since these are not permanent kill weapons. Once combat operations begin (or are imminent), the PRC would likely turn to destructive means like direct-ascent (DA) ASAT missile systems in an attempt to destroy our ISR satellites and permanently remove them from the fight.

In addition, PRC officials have publicly indicated their intent to acquire radiofrequency (RF) weapons as a means of defeating technologically advanced military forces. Chinese writings have suggested that RF weapons could be used against C4ISR, guided missiles, computer networks, electronically-fused mines, aircraft carrier battle groups, and satellites in orbit. An ASAT mission is undoubtedly one of the most stressing RF weapon applications. For a ground-based system beaming RF energy into space, very high power levels as well as a large high-gain transmitting antenna would be required. In contrast, an RF weapon delivered via a DA ASAT or deployed as an orbital system, would suffer severe constraints on system size and mass. Even if the Chinese commit significant resources to an RF ASAT development program, they are unlikely to be able to deploy such a weapon for at least fifteen years.

In conclusion, China has an aggressive space and counterspace program that is just one element of their comprehensive antiaccess strategy to degrade, disrupt, deny or destroy our ability to exploit our asymmetric advantage in information-enabled military operations. Continued Chinese investment in the design, development, deployment and employment of space and counterspace systems will increasingly challenge our traditional space dominance and could dramatically reduce our freedom of action in the event of a conflict in the region.

Cyberspace and China's Antiaccess strategy

Question

Explain the cyberspace related aspects of China's area control and antiaccess strategy. How might China's cyber operations degrade, disrupt, deny, or destroy U.S. military capabilities in the western Pacific in the event of a conflict between China and the United States?

Introduction

The word antiaccess does not appear in PRC writings, but PRC authors often reference sets of strategies designed to deny access to a physical space or information realm. Exploitation of the cyber realm can be used as an antiaccess or area control tool when cyber attacks or computer network exploitation is used to deny information to the enemy. Additionally, control and exploitation of the cyber realm is a key element of the Chinese information superiority strategy, which is an integral part of their overall antiaccess strategy. A key component of the PRC antiaccess strategy is denial of information to the enemy. Cyber capabilities can be used to deny information, either by network attacks or planting false information

Antiaccess Strategy

A Chinese antiaccess measure can be considered to be any action that has the effect of slowing the deployment of friendly forces into a theater, preventing them from operating from certain locations within that theater, or causing them to operate from distances farther from the area of conflict than they would normally prefer. Chinese writings suggest that key elements of a comprehensive Chinese strategy for defeating a military power like the U. S. would consist of actions designed to impede U.S. military access to the Asian theater in the event of a U.S.-China conflict. Writings emphasize "gaining mastery by striking first," possibly through surprise attack or preemption. This suggests that Chinese leaders might consider preemptively attacking U.S. forces as they are deploying to a region in what U.S. policymakers intend as an action to *deter* a conflict. Attacks on C4ISR targets have an antiaccess effect by disrupting the deployment of U.S. military forces to a region or by interfering with command, control, and communication or early warning capabilities to the extent that a decision would be made to withdraw forward-deployed forces farther from the locus of conflict. Attacks against C4ISR systems can involve operations against military and civilian targets in all five dimensions—land, sea, air, space, and cyberspace—and can be undertaken during peacetime and wartime.

Cyber warfare in an Antiaccess arena

The Chinese have identified the U.S. military's reliance on information systems as a significant vulnerability that, if successfully exploited, could paralyze or degrade U.S. forces to such an extent that victory could be achieved. According to RAND analysis, Chinese analysts believe that attacks against information systems can delay the deployment of U.S. military forces by disrupting communications or

denying the U.S. military access to information on enemy whereabouts. Chinese analysts note that information warfare can employ either "soft-kill" or "hard-kill" methods. Soft-kill methods include computer network attacks and electronic jamming, while possible hard-kill methods include directed energy weapons, explosives, and kinetic energy attacks. Cyber targets could include computer systems based in the U.S. or abroad, command and control nodes, and space-based ISR and communications assets. Noting the great distances that U.S. forces would need to travel in a conflict with China, attacks against logistics systems are also discussed. The goals of these attacks would be to delay the deployment of additional U.S. forces to the region and to render existing forces in the region less effective or more vulnerable by preventing timely supplies of the materiel needed for war-fighting.

The net result would be cyber warfare. Cyber warfare has the potential to terrorize, isolate, demoralize and cast a country into disarray. US military networks are constantly under siege, and in some cases, intruders, particularly China, have made off with militarily useful data, such as the terabytes of files stolen on the F-35 Joint Strike Fighter's electronics systems and designs. It is likely for malicious software to be lurking on military networks and remain hidden until the enemy's desired end state. However, cyber attacks are not just limited to the military, civilian networks in the US and countries which host our forward deployment bases can be hacked as well. These networks—electrical grids, communications, water supplies, banks and more—provide essential services to military installations and communities around the world and are critical to the day-to-day lives of millions more. While their impact on the military may seem indirect, any cyber attack which succeeds in creating widespread disruption on a national scale is certain to at least impede, if not debilitate military operations and critical military support functions.

Non-Traditional Strategies and the 'Three Warfares'

Question

Discuss other non-traditional strategies that the PRC could use to affect U.S. operations in the western Pacific, such as what the Chinese military calls the *Three Warfare's* (that is, psychological operations, influence operations and legal arguments).

Introduction

The PRC concept of *Three Warfare's* incorporates psychological, influence and legal arguments. These concepts are widely discussed in PRC literature and the open source press. The *Three Warfare's* concepts are part of what the U.S. has termed China's antiaccess strategy, a strategy to keep an enemy at bay through the development of technology, advanced weapons and information operations designed to keep an enemy out of certain areas, whether they be physical spaces or the information arena. Psychological, influence and legal arguments are not new concepts for the PRC but first appeared as a unified grouping in 2003. The PRC is currently conducting psychological operations, influence and legal operations in an effort to create a favorable environment for current and future PRC actions. Each of these types of operations, and their relationship to the concept of antiaccess, will be discussed below.

The "Three Warfares"

The *Three Warfare's* concept first appeared in 2003 in Chinese doctrinal writings. Since 2003, discussion of the *Three Warfare's* has been ongoing throughout PRC military writings as well as international media. PRC doctrine introduces the *Three Warfare's* concepts; psychological, influence and legal, as a way to describe and quantify military efforts to undermine a superior enemy's military abilities as well as influencing the enemy civilian leadership's 'will to fight'. Additionally, the *Science*

of Military Strategy, notes that "war is not only a military struggle, but also a comprehensive contest on fronts of politics, economics, diplomacy, and law." Each of the *Three Warfare's* concepts are separate, but intertwined and many actions that fall underneath these operations are taking place now as the PRC prepares and influences the battlespace in which they will fight future wars, whether kinetic or non-kinetic wars. Each of the *Three Warfares* concepts are further described below:

Psychological Operations (PSYOPS): According to PLA doctrinal literature, psychological warfare attempts to undermine military operations by conducting operations aimed at deterring and demoralizing military and civilian populations. PSYOPS includes radio, TV, propaganda, leaflets, deception and coercion operations. In the PRC, PSYOPS is also likely to be conducted against their own people (and most likely is already being conducted) to assure the population of Chinese success and insulate them from foreign sources and opinions. Psychological operations are also likely to be used in conjunction with other traditional means of warfare such as missile attacks, to increase the effectiveness of these types of kinetic attacks. Psychological operations can assist in seizing the initiative, conducting key point strikes, reducing the effectiveness of adversary strikes and achieving information superiority by overwhelming information flow or discrediting the available information.

The 2010 Annual Report to Congress: *Military and Security Developments Involving the People's Republic of China* defined psychological operations as: *seeking to undermine an enemy's ability to conduct combat operations through psychological operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.* The PRC can use psychological operations in conjunction with cyber attacks, by planting propaganda, and in conjunction with other non-traditional means such as jamming U.S. satellites. Psychological operations are also aimed at the civilian population in an effort to undermine civilian support. If aimed at Taiwan, they would likely target the Taiwan's leadership and appeal to the population, encouraging them to support reunification. Against the U.S., psychological operations would likely appeal to U.S. sentiment about international law and encourage U.S. civilians to oppose war in general, encouraging a diplomatic solution, thus delaying U.S. entry into the theater of operations. In the western Pacific, the U.S. is most vulnerable to PRC psychological operations against U.S. partners including South Korea, Japan and the Philippines. Should PRC psychological operations be successful, the U.S. risks losing basing or access rights to these locations, hindering our ability to operate in the region and furthering Chinese antiaccess goals.

Influence Operations: The 2010 Annual Report to Congress also defines influence operation, calling them: *operations aimed at influencing domestic and international public opinion to build public and international support for China's military actions and to dissuade an adversary from pursuing policies perceived to be adverse to China's interests*. Influence operations have also been referred to as media operations, or public opinion warfare. Although this concept sounds very similar to psychological operations, it differs fundamentally in what the operation attempts to affect. Influence operations focuses on both public and international opinion to support Chinese military actions through the controlled release of information. The PRC is conducting influence operations now through their censoring of the internet, monitoring of PRC bloggers and controlled release of both military and civilian information to the international media. The recent information release of the new Chinese J-20 fighter is a prescient example of just such an operation.

In a conflict with the U.S. or another adversary, the PRC is likely to use the media to control information flow. They will likely manipulate images to show only what they want seen and will actively block content from the internet. Media warfare also focuses on influencing the countries own population through management of public opinion. Media warfare selectively targets audiences and differentiates between internal and external audiences. The PRC conducts influence operations on a daily basis through media management, state owned newspapers and television stations, censorship and self-promotion of Chinese ideals. Additionally, media warfare is central to both psychological and legal arguments through reinforcing of opinions using the international and domestic media.

Legal Arguments: The PRC uses legal arguments to manipulate international law to their advantage and to legitimize Chinese actions. Legal warfare was defined in the most recent Annual Report to Congress as: *using international and domestic laws to gain international support and manage possible political repercussions of China's military actions.* These arguments include using forums such as the United Nations to argue their claims, claiming their own rights have been violated or insisting that all issues are domestic issues and therefore not of concern to outsiders.

Additionally, the PRC is becoming very adept at using this tactic in the South China Sea, reiterating through media operations China's core interest and historic presence in the South China Sea. Additionally, the PRC is focusing on desensitizing the international community to their presence in these areas by monitoring, and shadowing, international sea traffic, aggressively managing the air space and consistently patrolling the seas, especially the Chinese exclusive economic zone (EEZ). Additionally, the Chinese response to the sinking of the South Korean naval vessel, the Cheonan, and the resulting calls for a diplomatic solution indicate China's use and understanding of the international system. China is very adept at using the international forums to avoid incidents. In the event of a conflict with Taiwan or any other adversary, the PRC will likely manipulate the international legal system to their own advantage, claiming sovereignty, right of defense or interference by an outside party as illegal. They will use the international arena to legitimize their actions, and will also use their economic and diplomatic power (through ASEAN or the UN) to coerce other smaller Asian states or larger trading partners to support, or maintain a neutral opinion, on their actions. Lastly, the PRC has watched and learned from the U.S.'s experience with claiming legal warfare within the international community and most likely will attempt to do the same thing should they conduct kinetic or non-kinetic warfare. The actions they are taking now support their current and future actions.

The "Three Warfares" and Antiaccess

Antiaccess and the concept of the *Three Warfares* are often used in conjunction but are actually separate concepts. The *Three Warfares* is a unified concept falling under an information superiority campaign. The term antiaccess is typically used to describe a set of PRC capabilities (military, economic and diplomatic) or a linkage of concepts that can be used to deny access to a specific area or arena. The word antiaccess is not used on PRC doctrinal writings, but PRC writers often reference sets of strategies designed to deny access to an area, either a physical or information space. Documents often refer to strategic goals or *assassin's mace* technologies (specific advanced technologies with great deterrent capabilities such as anti-satellite or anti-ship ballistic missile technologies) and make specific claims about capabilities that would allow the PRC to seize the initiative in a conflict. The capabilities the PRC refers to in discussions include both traditional and non-traditional capabilities including ballistic missiles and fighter aircraft (traditional) and cyberspace, space warfare and information operations (non-traditional) and under which the *Three Warfares* concepts can be found.

The concept of antiaccess first emerged in U.S. strategic writings in the early 1990s, but is still not defined as of the most recent update (December 2010) to the JP 1-02, DOD Dictionary of Military and Associated Terms. RAND defines an antiaccess measure as: *any action by an opponent that has the effect of slowing the deployment of friendly forces into a theater, preventing them from operation from certain locations within that theater, or causing them to operate from distances farther from the locus of a conflict than they would normally prefer*. This is a decent definition, although it refers mainly to capabilities and ignores the strategy portion of antiaccess. Overall, an antiaccess strategy encompasses all the capabilities, both military and civilian, that a government has at their disposal in order to deny an enemy access to a given space, or arena (including economic, diplomatic, military, media or a land or sea mass) during a time and space of their choosing. The *Three Warfare's* concept put forth by the PRC is an element of their information superiority campaign *and* antiaccess strategy.

> *"An essential element, if not a fundamental prerequisite, of China's emerging antiaccess/area-denial regime is the ability to control and dominate the information spectrum in all dimensions of the modern battlespace."*
>
> *- DOD ANNUAL REPORT TO CONGRESS: Military and Security Developments Involving the People's Republic of China, 2010*

In conclusion, the PRC *Three Warfares* concepts are a fundamental part of the overall information superiority strategy. Information superiority is also a fundamental piece of the PRC's antiaccess strategy. Psychological operations, influence (media) operations and legal arguments are concepts well understood by PRC leadership. The PRC is particularly adept at influence operations through the use of the internal and external media and their ability to control information. They are also increasingly using and exploiting the legal arena. Psychological operations are more subtle, and currently are primarily targeted at the island of Taiwan, attempting to deceive and confuse Taiwan's civilians and military alike through broadcasts, controlled information leaks and even the positioning of weapons directly across from the island. The *Three Warfares* incorporates many traditional and non-traditional methods of warfare, often combining subtle and obvious signals for maximum effect. We can expect the PRC to mature capabilities in these concepts in the future, supporting their overall campaign for information superiority and thus their antiaccess goals as well.