

Testimony
U.S.-China Economic and Security Review Commission
China's Military Modernization and its Impact on the United States and Asia Pacific Region
March 30, 2007
James A. Lewis
Center for Strategic and International Studies

Let me thank the Commission for the opportunity to testify. I would like to talk about changes in the nature of warfare, the implications of these changes for China's military modernization, and the nature of the challenge these changes pose to the U.S. and others.

A discussion of these issues would need to consider China's intentions and capabilities. China's intentions are unclear – the policy processes in Beijing are opaque when they are not impenetrable, but we can make deductions about these intentions by observing the kinds of military capabilities China is acquiring. There needs to be some care taken in making these deductions - modernization could reflect military ambitions, a desire for improved defense, a wish to demonstrate prestige and status, or a combination of all of these. Any estimate of the effect of China's military modernization also needs to consider the strengths and vulnerabilities of potential opponents, and in particular the U.S.

We should consider China's military modernization in the context of changes in the nature of warfare. Three related developments shape the environment for armed conflict. The first is the development of a high tech, information-intensive style of combat pioneered by the United States in the first Persian Gulf War. The second is the reaction of our potential opponents to the conventional military superiority this high tech, information intensive mode of combat has given the U.S. The third is the development of new kinds of weapons and new modes of attack. In combination the conventional strength provided by the high tech, information intensive style of combat adopted by the U.S. means that potential opponents would seek asymmetric advantage – avoiding conflict where the U.S. is strong and attacking where the U.S. is weak, and they will use unconventional weapons and tactics in doing this.

Modernization

These trends explain some of what China is doing in its military modernization efforts, but they are not the full explanation. China appears to be deeply concerned with prestige, with gaining international recognition that it has reclaimed its place among the great nations of the world. China would also like to be recognized as the paramount power in the Asia-Pacific region. Some of its activities and acquisitions are made in the interests of prestige and influence, and the competitors for China in these efforts include not only the U.S. but also China's powerful neighbors; India, Russia and Japan.

China's military was, for many decades, very poorly adapted to the high tech style of combat that began to appear in the 1970s. A decade ago, China's military lagged behind the larger powers, such as India. More embarrassingly, it also lagged behind smaller countries like Korea or Singapore in the sophistication of its arsenal. China's national policies to develop a high tech economy, with efforts like the 863 Program, have always had a military component in order to remedy China's lag in military technology.

There has also been a theme for many decades in Chinese policy and thinking of 'catching up' to the west or even 'leapfrogging' western nations. The notion that China would be able to find some way to surpass other nations remains attractive in China, despite the many failed

leapfrogging efforts, and it reinforces Chinese thinking about the need to gain asymmetric advantage.

China's military modernization programs was at first an effort to repair the damage done by Mao's romantic notions of combat and to build the forces needed to deter potential attackers. It is now an effort to assemble the forces needed to assert regional primacy. China's likely goal in this modernization is to build military forces that are superior to its regional peers, that create the option for quick and successful action against Taiwan, and that are capable of defeating U.S. forces in a regional contest.

These are not easy goals to attain, however. India, Russia, Japan, and even Korea all have formidable military forces. U.S. forces far surpass these nations in their capabilities, and even though the war in Iraq has seriously eroded U.S. ground force capabilities, U.S. air and naval forces remain superior to China or any other nation. Nothing China has done in its modernization efforts changes this. Reaction to China's programs, particularly in Japan, means that the goal of regional supremacy is probably unattainable, but this does not mean the Chinese will stop their pursuit of it.

Asymmetric Warfare

China is not at all likely to stop its pursuit of capabilities that counter U.S. strengths. China's military is not a peer to the U.S., but it is a challenger. The challenge comes from a combination of increased conventional capabilities and from the pursuit of asymmetric advantage – using new weapons and tactics to attack an opponent in areas where it is weak or vulnerable. Seeking asymmetric advantage is not new, nor is China the only country to seek it. What is new is the means that U.S. opponents like China and others plan to use to gain asymmetric advantage. One part of the modernization effort looks for ways to counter U.S. force projection capabilities. Other modernization efforts look for ways to erode the U.S. military advantage by attacking information and communications assets, including satellites and networks.

China's military is developing weapons and tactics to produce this erosion. The most dangerous of these programs are those aimed against U.S. carriers. China has acquired many of the technologies developed by the Soviet Union to attack U.S. Carriers and it is refining these technologies and the tactics needed to use them. Another set of programs is developing anti-satellite capabilities and a third involves information operations. While China has expended considerable effort on anti-satellite weapons and information operations, neither activity poses much risk to U.S. military superiority.

Anti-Satellite Weapons

China's January 2007 anti-satellite test has received much attention. The test should not have been a surprise. The Chinese have been working on anti-satellite weapons for at least a decade, despite their denials. The particular weapon used in the test – a kinetic intercept of a low earth orbit satellite - is the least sophisticated mode of anti-satellite attack, and something that the Soviets and the U.S. developed, tested and abandoned decades ago.

China is working on other anti-satellite weapons, and public reports speculate that these include ground-based lasers and, perhaps, attack satellites. It also includes cyber attacks against the ground facilities and networks that control U.S. space assets. Since it is clear to most militaries that a good portion of the U.S. advantage in combat comes from satellite data,

potential opponents like China are searching for ways to interfere with these services from space and the networks that support them.

As with many of China's military modernization programs, a robust U.S. response can undercut China's efforts. In anti-satellite weapons, the U.S. can reinforce its advantage in space by continuing to harden its satellites, by moving to a more flexible military space architecture, by accelerating its Operationally Responsive Space programs and by developing alternative technologies, such as high-altitude UAVs and mini-satellites. These alternate technologies could provide 'space-like' services that would render attacks on satellites useless. Since the U.S. is already pursuing many of these programs, and given the robustness of its satellite fleet, if the Chinese were to use anti-satellite weapons in a clash, they would gain no advantage. It is in the U.S. interest to ensure that this continues to be the case.

Prior to the test, many nations, including China, castigated the U.S. for its plans for future military activities in space. The U.S. ignored them, and this has proven to be the right decision. Space arms control efforts would not help the U.S. retain its military advantage, nor would they make a positive contribution to national security. A UN treaty banning weapons in space would harm U.S. national security. We would observe it; others would not. One reason China has been an advocate of a treaty is because it calculates that an agreement would put the U.S. at a disadvantage.

A ban would be unverifiable, even if there were an inspection regime put in place. There are many ways to attack satellites and the services they provide, and the kinetic weapon China used is the most primitive and most detectable means of attack. No treaty could credibly address all of them. It is difficult to negotiate seriously with a partner who has little experience of arms control and whose credibility, after years of denying that it had anti-satellite programs and asserting that its intentions in space are entirely peaceful, is badly tattered. Space is an area of U.S. military advantage – asymmetric advantage in that no other nation can match it. One way to counter China's military modernization is to continue to pursue aggressively the U.S. asymmetric military advantage in space.

However, anti-satellite weapons might not pose the greatest problem for the military space services used by the U.S. military. We should also assume that the Chinese are putting considerable work into deception and denial efforts, including jamming of satellites signals, interference with networks, and spoofing of targets. This can involve, for example, carefully studying the signature of a target weapons system that the U.S. sensor collects, and then duplicating that signature in a decoy. Denial and deception efforts may actually be of greater concern, since we know from the experience in Kosovo that a skilful combination of concealment, mobility and deception can confuse U.S. technical collection.

Informational Warfare

Denial and deception are one aspect of information warfare. The data collected by sensors is erroneous, making the decisions based on that data also erroneous. Another information warfare tactic would be to corrupt stored data, or to damage the computer networks that process and distribute data and support decision-making. Like satellites, China has targeted U.S. information systems as a vulnerable component of the U.S. style of combat.

Information technologies are a primary target for asymmetric attack. Information – an array of intangible goods that include technological know-how, data, statistics, and news, and the networks and processing technologies that aggregate, process and distribute it have become

an integral part of national power. Gaining information superiority, whether through knowing more than an opponent or from disrupting his ability to know, has also become one of the keys to success in conflict.

Conflict in cyberspace is clandestine, so it can be difficult to assess intentions and risks. It is easier to assess the vulnerability of U.S. systems and the potential consequences of an information attack. U.S. networks are very vulnerable. Even highly sensitive networks used for command and control or intelligence are not invulnerable. From an intelligence perspective, several nations, including China, have exploited the vulnerabilities to gain valuable information. These foreign intelligence efforts and the feeble U.S. response have damaged U.S. national security. It is safe to assume that in the event of a conflict, a foreign opponent would also attempt to exploit our vulnerable networks in an attempt to disrupt and damage our military operations.

The central point to consider in this assessment of cyber vulnerability and the consequences of cyber attack is the linkage between information systems and military capability. If U.S. military capabilities depend entirely upon information systems, cyber attacks will greatly do considerable damage. If there is redundancy in information systems or if networks are resilient (e.g. they recover quickly), cyber attacks will not do much damage. For the U.S., so far, vulnerability in a computer network does not automatically translate into a loss of military capability. The risks and consequences of cyber attack are routinely overstated in the popular press, and cyber attack will not provide China with a decisive military advantage.

One way to assess this risk is to ask whether a cyber attack by China launched a few days in advance of a clash could prevent U.S. carrier battle groups from deploying to the Taiwan Straits. Launching the attacks too early would create the risk of discovery and countermeasures. China could attempt to interfere with telecommunications systems – although a successful effort would have to simultaneously disrupt land lines, cellphones, the internet and satellite communications – a next to impossible task. China could attempt to interfere with transportations, ranging from air traffic control to traffic signals to make it more difficult for the crews to assemble, although it is hard to see what a cyber attack could add to the gridlock and overcrowding that occurs routinely on bad days. It could attempt to interfere with the electrical grid, which could complicate and slow a ship's departure. Hackers could take over broadcast radio and TV stations, and play Chinese music and propaganda, or change broadcast parameters in an effort to create radio interference. But these sorts of annoyances do not provide military advantage.

China could attempt to interfere with the computer networks that support logistics and supply chains, but since any clash is likely to be a come-as-you-are conflict, there would be no immediate effect. The Chinese could attempt to disrupt critical infrastructure. This also would not seriously affect the deployment of U.S. forces, but it could hold the risk for China of widening any conflict in exchange for very little benefit. An attack against U.S. civilian infrastructures could easily prompt retaliatory measures. Surreptitious, long term cyber attacks on the U.S. economic system might seem attractive as a way to weaken the U.S. before a conflict, but the uncertain benefits of such attacks – and they are uncertain because the attacks might not work and are as likely to damage China's economy along with any harm done to the U.S. - would have to be weighed against the serious risk and damage that would occur if the effort was discovered.

Again, robust U.S. preparations can mitigate the consequences of a cyber attack or a campaign of deception. If the U.S. plans for how it can continue to operate even though its information systems are under attack, if it builds redundancy and resiliency into those

networks that are important for military performance, it can greatly reduce the risk of cyber attack by China or other potential opponents.

A better strategy for informational warfare would be to seek to increase an opponent's uncertainty. Increasing uncertainty in the mind of opposing commanders degrades that opponent's effectiveness. Denial and deception leaves opponents certain that they know what is happening when, in fact, what they believe is wrong. An uncertainty strategy makes an opponent unsure that they know what is happening. Finding ways to inject false information into the planning and decision processes of an opponent, or manipulating information that is already in that system to make it untrustworthy, can provide considerable military advantage. There is reason to believe that the Chinese now use false or misleading information to manipulate and confuse their opponents. We should not discount the possibility that China will pursue an informational strategy that seeks to expand uncertainty and confusion instead of attempting to unleash an improbable 'electronic pearl harbor' that offers only uncertain results.

Miscalculation

This assessment of the risk posed by China's development of unconventional weapons and tactics downplays the effect of cyber weapons or anti-satellite weapons on the military balance between China and the U.S. It is important for all concerned to remember that in the same period that China has been modernizing its military forces, the U.S. has also made significant improvements to the capabilities of its own forces and that these efforts at improvement continue. These U.S. improvements increase the likelihood of success in any conflict, and, if used correctly, will deter opponents from even beginning conflict. There is however, one area of risk that deserves greater attention.

That is the risk that the Chinese government will miscalculate the U.S. response and the international reaction to a military adventure, and that they miscalculate the benefits and effect on the military balance of anti-satellite or cyber weapons.

The Chinese clearly miscalculated the reaction to the anti-satellite test. This miscalculation reflects a degree of parochialism in Chinese security policy, a lack of experience in international politics and a certain degree of hubris, perhaps justifiable, over China's tremendous economic success. Whatever the reasons, they did something that a more experienced nation might have decided against doing.

This makes it fair to ask if the Chinese could similarly miscalculate the balance of power in the region. It is not inconceivable that they could overestimate the advantages provided by asymmetric attacks and overestimate the exhaustion of U.S. forces because of Iraq. We can think of several incidents in the past - in 1914 or 1941, for example - when authoritarian regimes have made such miscalculations and initiated conflicts that appeared unthinkable. While it is unlikely that China would make this sort of miscalculation, particularly before the 2008 Olympics, it would benefit the U.S. to make clear to all of its potential opponents that asymmetric attacks are 'second best,' unlikely to degrade U.S. military capabilities, or change the likely outcome of any clash.

In a rational and transparent world, such miscalculations would not occur. While we do not live in such a world, the U.S. can take actions to decrease both the risks of miscalculation and the risks of asymmetric attack. We cannot prevent China's military modernization but the right policies will let us manage any risk that modernization poses.