Asymmetric warfare and the People’s Republic of China (PRC) have something in common. Both are part of the debate over what the preeminent threat to American power will be in the twenty-first century. Some say asymmetric warfare has displaced traditional combat; others view this as a dangerous exaggeration. Likewise, some see China’s ascension as relatively benign or beneficial even as others label it the United States’ biggest future security concern. As China has become a global economic powerhouse, it has also devoted increasing amounts of resources towards modernizing and improving its military. In the eyes of those wary of China’s growing military power, its capabilities for waging asymmetric warfare are one of the greatest causes for alarm.

Broadly defined, asymmetric war is a conflict between belligerents with a substantial difference of relative power in which the weaker party uses unconventional methods to undermine an opponent’s advantages. The weaker side targets specific vulnerabilities and exploits them in order to level the playing field. Asymmetric warfare holds an important place in Chinese military thought. Recent efforts to modernize have emphasized the development of asymmetric capabilities, especially the capacity for information warfare. This is one of the most important dimensions of China’s rise. The United States is almost certain to maintain conventional military superiority over China in the foreseeable future. However, asymmetric war is a potential instrument for China to diminish the value of this superiority.

It is important not to overstate the threat of asymmetric war. The PRC is far from posing a serious global challenge to the United States. It is unlikely that asymmetric power would allow China to challenge and defeat American hegemony. That said, asymmetric war is not an
imagined risk. Asymmetric power will be a significant factor determining outcomes in the limited-scale and limited-stakes military conflicts most likely to involve China (such as over Taiwan). It is crucial that the threat of asymmetric war with China be neither exaggerated nor ignored.

First, I explore the concept of asymmetric warfare in general, looking at what potentially falls under this classification and how weak actors have employed it against strong actors. With this foundation, I then turn to classical and modern Chinese theoretical work on this subject. Next, I examine China’s current capacity for waging asymmetric war. Finally, I evaluate the threat of asymmetric warfare in the specific context of potential conflicts with China and conclude with a few implications for policy.

**The “New” Generation of Warfare**

Asymmetric warfare is commonly defined as using unorthodox methods, tactics, and strategies that focus one’s strengths on an opponent’s weaknesses to undercut any advantages that the enemy has. The idea applies to conventional realms of combat (air, ground, sea) but also includes unconventional categories such as information, legal, and ecological warfare. Asymmetric approaches are uncommon, innovative, and often cannot be mirrored by the other side. Such approaches are designed to turn an enemy’s strengths against them by exploiting particular weak points. The principles behind asymmetric warfare are not new. Such concepts can be found in many historical texts including Sun Tzu’s *The Art of War* (covered later in this paper), Machiavelli’s *The Prince*, Miyamoto Musashi’s *A Book of Five Rings*, and Carl von Clausewitz’s *On War*. However, recent connections between technology and asymmetry have
led to increased conceptualizing of this type of combat as a new generation of warfare, distinctly different from traditional conflict.¹

There are two broad connections between asymmetric warfare and technology. The first is that, for all its benefits, modern technology carries serious and inherent risks. For example, the terrorists that carried out the November 2008 attack in Mumbai used Google Earth to familiarize themselves with the city then coupled their guns and explosives with mobile phones and the global positioning system.² The pervasive and ubiquitous nature of the internet – despite the positive effects of increased communication and information flow – comes with a corresponding susceptibility to cyber attacks and hacking. The United States’ leading edge in, and dependency on information technology (IT), makes it one of the most vulnerable countries to asymmetric information attacks.³ The second connection is that advanced technology provides additional capabilities for asymmetric warfare. For example, highly advanced information systems offer the average hacker immense power to carry out cyber attacks on government mainframes. These links between technology and asymmetric warfare have become more prominent in recent years.


because of the revolution in military affairs (RMA) that has applied modern engineering and science (especially in IT) to the design and use of weapons.\textsuperscript{4}

Asymmetric conflicts are often characterized by a considerable difference in relative power between or among the combatants. Because the stronger side possesses a conventional advantage, usually due to greater manpower and material resources, the weaker side cannot hope to win through conventional means. For this reason, weaker combatants generally look to unconventional methods to attack their enemy by exploiting certain weaknesses. These vulnerabilities can be military ones. As Thornton notes, one such example is using an anti-ship cruise missile (ASCM) “costing some hundreds of thousands of dollars... [to sink]... ships worth hundreds of millions of dollars.”\textsuperscript{5} The vulnerability can also be political or psychological. The U.S. effort during the Vietnam War greatly suffered from the guerrilla war fought by the Viet Cong not just because of tactical or strategic difficulties, but also because the guerrilla war lengthened the timeframe of the conflict. This slowly drained the political will from the American administration and shifted public opinion against the war.\textsuperscript{6}

What connects the exploitation of military and political/psychological weaknesses together is that small-scale actions are leveraged to have a proportionally large strategic impact. Consider the September 11 attacks: a small group of terrorists armed with box cutters destroyed the twin pillars of America’s economic power with four airplanes, killing nearly 3,000 people and striking the nerve center of the American public. Conceptions of asymmetric warfare sometimes include the notion that an entire society is the target, eliminating the distinction

\textsuperscript{5} Thornton, \textit{Asymmetric Warfare}, 107.
between civilian and military.7 Terrorists are seen by some as the “archetypal asymmetric adversary” because they are weak, dispersed, often lacking in numbers and resources, and constantly seeking to derive large strategic effects from small actions.8

The strategic use of air, land, and naval power can also fall under asymmetric warfare if these traditional approaches are used in ways that cannot be easily mirrored. Anti-aircraft artillery, underwater torpedoes, armor piercing rounds, and precision-strike ballistic missiles are all effective ways to bypass the battlefield advantages offered by jet fighters, tanks, and aircraft carriers.9 The stronger side cannot employ these same tactics because their opponents do not generally possess the advantages of having this advanced equipment in the first place. The employment of information warfare (IW) tends to be inherently more asymmetric. Although conceptions of IW vary among scholars and analysts, it can broadly be thought of as a holistic approach to fighting that manipulates information in a manner constituting an offensive strike or defensive move against an enemy.10 Information warfare is best described as an umbrella term that encompasses a variety of disciplines, including deception, psychological operations, electronic warfare, cyber warfare, and network-centric warfare.11 What is especially important about IW is that both capacity for usage and vulnerability to it are functions of reliance on information technology. For example, the Russian military invasion of Georgia in 2008 was

---

7 Jones et al., Global Information Warfare, 4.
8 Thornton, Asymmetric Warfare, 25.
9 Ibid., 80-81, 103-104, 127.
10 Ibid., 56-57.
11 Electronic, cyber, and network-centric warfare are related but distinctly different from each other. Electronic warfare (also sometimes called electromagnetic warfare) relies on using the electromagnetic spectrum as a defensive and offensive tool: electronic jamming, stealth, radar deflection, high energy radio frequency weapons (HERF), and electromagnetic pulse (EMP). Cyber warfare (also called computer network warfare) involves the use of hacking, viruses, Trojan horse programs, and other methods of infiltrating, damaging, and protecting information stored on computers and the internet. Network-centric warfare seeks to translate information dominance into military superiority (generally through solid networking of geographically dispersed military forces). See Yoshihara, Chinese Information Warfare, 3-5, 17; Clay Wilson, “Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,” in Cyberterrorism and Computer Attacks, ed. Lawrence V. Brown (New York: Novinka Books, 2006), 3-6; Thornton, Asymmetric Warfare, 54, 134-135.
accompanied by a coordinated barrage of cyber attacks. While these attacks were mostly a nuisance, the 2007 cyber assault on Estonia was much more devastating since Estonia has a much greater reliance on the internet and information technology.

Although weak actors generally rely on asymmetric approaches more than strong actors, this form of warfare is not exclusive to one side. Russian cyber warfare is one example of this. The United States has also long recognized the importance of the internet as a weapon and has placed emphasis on developing the capacity for computer network warfare. This capacity is dependent on information dominance and thus intimately tied to the development of information technology, which the United States is a global leader in. Advanced sensor equipment and electronic jamming units allowed the United States to detect Iraqi forces in sandstorms and undermine enemy communications during the invasion of 2003. In addition, the U.S. has applied asymmetric principles to traditional military capabilities. Early into the Gulf War of 1991, the United States used cruise missiles to make precision strikes on key targets which destabilized the electronic network of the Iraqi air-defense system.

Recognizing that strong actors can use asymmetric warfare is important. It is easy to think of asymmetric approaches as exclusively used by the weak against the strong. While it is true that the weak generally rely on these approaches more often, the strong can also employ them to their advantage. Ivan Arreguin-Toft’s distinction of direct and indirect strategies is useful here. Direct strategies attempt to destroy the capacity to fight by capturing an enemy’s

---

15 Paarlberg, “Knowledge as Power,” 129-133.
17 Ibid., 320-321.
resources (e.g. capital city, bridge, fort) while indirect strategies seek to destroy the capacity to fight by inflicting pain, disrupting peace of mind, and destroying values.\textsuperscript{18} The specific strategies that fall under direct and indirect do not exactly line up with those that would fall under traditional and asymmetric (e.g. strategic bombing is direct but it could be classified as asymmetric). However, Arreguin-Toft’s key insight is that for weak actors the ideal counterstrategy to a direct approach is an indirect one. Opposite-approach interactions are likely to favor weak actors by protracting the conflict and mediating the relative power difference.\textsuperscript{19} Rather than conceive of the distinction between asymmetric and traditional warfare as a weak-strong dichotomy, it may be more appropriate to think of the relationship between strategy and effective counterstrategy.

\textbf{The Theory of Chinese Asymmetry}

Ideas of asymmetric warfare have been present in Chinese military thought since ancient times. These ideas are perhaps best expressed in the writings of Sun Tzu and the less-well known Sun Pin.\textsuperscript{20} In \textit{The Art of War}, Sun Tzu discusses the importance of combining orthodox and unorthodox methods, as well as targeting an adversary’s weaknesses with one’s strengths to achieve victory.\textsuperscript{21} Some central tenets of information warfare are present, seen especially in his emphasis on controlling information through the use of deception and the employment of spies.\textsuperscript{22}

\textsuperscript{18} Arreguin-Toft, “How the Weak Win Wars,” 104-107.
\textsuperscript{19} Ibid., 107-110., 121-123. Arreguin-Toft notes that strong actors can win same-indirect-approach conflicts with weak actors if the former use strategies that are militarily effective but politically dangerous (such as barbarism against guerrilla warfare if the goal is long-term political control). This is different from certain asymmetric approaches, such as electronic warfare, which are both militarily effective and politically viable.
\textsuperscript{20} Sun Tzu and Sun Pin are more properly transliterated as Sunzi (Sun Zi) and Sun Bin. For the sake of simplicity, I keep my transliterations of author names uniform with the particular sources that I referenced. I write Mao’s name as Mao Zedong in the paper because this is the standard spelling today. However, I include Mao Tse-Tung in my citations to match the particular source I used. Regarding the works of Sun Tzu and Sun Pin, both were originally called the \textit{Sun Zi Bing Fa} and the \textit{Sun Bin Bing Fa}. Both can be translated simply as the art of war. However, the copies of the sources that I used were titled \textit{The Art of War} and \textit{The Art of Warfare} respectively. I preserve this distinction to keep the titles uniform to the referenced sources.
\textsuperscript{22} Ibid., 49, 168-172.
Sun Tzu conceives of military strategy as a holistic philosophy of defeating an enemy. He stresses constant adaptability to the changing conditions of battle. Just as “the form of water is to avoid the high and go on the low... [t]he form of a military force is to avoid the full and attack the empty.” Sun Pin’s *The Art of Warfare* discusses and expands on many of these same points. He accentuates the importance of understanding the “Tao” of achieving victory and avoiding defeat. The path to victory is not straightforward. It is holistic, dynamic, and in tune with nature. This translates into a mastery of discerning the reality on the ground, adapting to changing conditions, perceiving where an opponent is weak or in disarray, and learning how to commit a focused attack on weak points in order to gain a quick advantage. The strategy when facing a stronger opponent is to “attack where he is not prepared and go by way of places where it would never occur to him you would go.”

Other classical writings provide insights into effective methods of asymmetric combat. T’ai Kung focuses on how to employ “unorthodox armies” and the environment against a stronger adversary. Another places greater weight on evaluation of the enemy’s condition, striking only when there are clear weak points and exploitable circumstances of confusion and disorder. Such strategies is designed to yield greater results with less effort. One running theme in many classical texts is the comparison of military power to water. A successful army is one that can make itself into “the softest and weakest of things” yet overwhelm an opposing force

---

23 Ibid., 112.
25 Ibid., 137.
solely because “its nature is concentrated and its attack is totally committed.” The analogy to water implies how “the soft can control the hard [, and] the weak can control the strong.”

The legacy of this asymmetric thinking was carried on in more recent times by Mao Zedong. He understood that insurgencies and guerilla campaigns were fought for the support of the people. Those who won the hearts and minds of the people would be victorious even against a superior fighting force. In some ways, Mao also acted as a precursor to modern Chinese asymmetric thought. Although his perception of asymmetric approaches did not yet incorporate the revolution in military affairs of modern science and technology for use by the weaker side, he did recognize that defeat was inevitable as long as “native forces [fought] with inferior weapons against modernized forces on the latter’s terms.” The last part of this statement is significant, indicating his realization that weaker forces needed to adopt strategies that the enemy could not easily mirror. The weak had to find a way to fight battles on their terms.

Although talk of asymmetric combat, information operations, and intellectual warfare has been growing in China over the past couple decades, a watershed moment in Chinese military theory was the publication of *Unrestricted Warfare* in 1999. This book, written by two senior colonels in the People’s Liberation Army (PLA), is perhaps the first fully systematic outline of how weaker powers can use methods of warfare transcending all limitations and boundaries to defeat stronger powers. The authors advocate the use of financial warfare, terrorism, management of the media, control of natural resources, and manipulation of international law as strategies for defeating an opponent. Employing asymmetric power effectively allows one to

---

develop situations to one’s preference and liken the conventionally superior power of the enemy to “a big elephant charging into a china shop.”\textsuperscript{32} Although parts of the book border on almost complete fantasy, the text is useful because it marks the evolution of Chinese thought on asymmetric warfare.

Modern Chinese thought on asymmetric warfare has also more fully developed the concept of holistic warfare. Two of the foremost generals in the PLA have espoused a variety of information operations, including intelligence warfare, electronic strikes, and cyber attacks as necessary means for weakening the “enemy’s information center of gravity... and reduc[ing] his holistic combat efficiency.”\textsuperscript{33} Organizations outside the military have also contributed to theories of unorthodox warfare. When Chang Mengxiong worked as a senior engineer at the Commission for Science, Technology, and Industry for National Defense (COSTIND), he researched and advocated asymmetric approaches in which “the inferior could defeat the superior” through information based combat methods.\textsuperscript{34} Such approaches involve the combination of “high-tech and low-tech weapons” (e.g. electronic strikes and AK-47s) and utilizing nontraditional forms of warfare such as economic or political along with military power.\textsuperscript{35}

Chinese military thought has evolved from focusing on Mao’s concept of a “People’s War” to local conflicts fought with advanced technology.\textsuperscript{36} Ironically, it was the Gulf War of 1991 – when the United States demonstrated its unrivaled military strength – which forced a paradigm shift for many of the PLA’s older thinkers who still emphasized the role of man over

\textsuperscript{32} Ibid., 212.
technology. The preponderance of American power, and more specifically its reliance on advanced weaponry and information technology, led to the adoption of Local War under Modern High-Technology Conditions (LWUMHTC) as the dominant doctrine in the PLA by the mid-1990s. This adoption also stemmed from former paramount leader Deng Xiaoping’s belief that it was precisely these local conflicts which China would face in the future. Deterring these conflicts from erupting, or winning them if they do, requires building the capacity for initiative action, offensive striking power, and joint operations. To all of these, IW is a powerful supplement.

Major centers of IW research include the Academy of Military Sciences, the PLA Academy of Electronic Technology, COSTIND, and China’s National Research Center for Intelligence Computing Systems. China recognizes that the United States is far ahead in terms of military power and advanced technology. As a result, the Chinese have focused not only on offensive IW asymmetric advantages favoring a weaker party, but also evaluating and improving China’s underdeveloped IW defense in relation to technologically advanced rivals. It is America’s strength in the form of openness and access to information that provides an appealing weak point for exploitation.

**China’s Capacity for Asymmetric War**

Evaluating China’s asymmetric capabilities is difficult. Even the best intelligence and research is unlikely to uncover the details of secret programs developing information warfare. The publication of various defense white papers may provide a measure of this development. However, it is important to keep in mind that white papers also mislead by providing false

---

37 Ibid., 184-186.
39 James C. Mulvenon, and Richard H. Yang, eds., *The People’s Liberation Army in the Information Age* (Santa Monica: RAND, 1999), 179
information and decontextualizing particular facts. Furthermore, China has no incentive to “show its hand” as asymmetric power also incorporates and capitalizes on the element of uncertainty.\textsuperscript{41} That said, there are numerous accounts from governmental and non-governmental sources of China’s investment in information warfare. China’s development of conventional military power also suggests likely asymmetric applications in a variety of ways.

According to the U.S Department of Defense, China has invested in electronic countermeasures (such as angle reflectors and false target generators) and computer network operations (CNO)\textsuperscript{42}. IW is primarily a tool for disrupting the enemy’s information systems supporting combat capacity and power projection by achieving “electromagnetic dominance” in the early stages of a conflict.\textsuperscript{43} According to Larry Wortzel, the commissioner of the U.S.-China Economic and Security Review Commission, the PLA has established information warfare units to develop offensive and defensive capabilities in both electronic and cyber warfare.\textsuperscript{44} Such capabilities include viruses to attack enemy computer systems and networks, HERF weapons and EMP devices, and measures for computer defense. Chinese cyber attacks on American computer networks have been a significant problem in recent years.\textsuperscript{45} A number of cyber attacks on the Pentagon have been traced to China.\textsuperscript{46} While there is little evidence that Beijing is masterminding these attacks, it seems naïve to think there is no tacit consent from the

\textsuperscript{41} Thornton, \textit{Asymmetric Warfare}, 65.
\textsuperscript{43} Ibid.
\textsuperscript{45} These attacks include “Titan Rain,” an alleged group of hackers that broke into the mainframes of Lockheed Martin, Sandia National Laboratories, the Redstone Arsenal military base, and NASA. See Nathan Thornburg, “The Invasion of the Chinese Cyberspies,” \textit{Time Magazine}, September 5, 2005.
government. Some believe that the PLA has fostered a “cadre of hackers” and cyber warfare training schools for strengthening their IW infrastructure.\(^{47}\)

Although some of this progress parallels that made in other countries, what stands out to many is the comparatively greater scale and comprehensiveness of China’s programs.\(^{48}\) The first organized cyber warfare units appeared in the PLA in 2003 and have since become highly active and sophisticated components of ground force organization.\(^{49}\) In 2005, the PLA started incorporating offensive CNO into its exercises, focusing primarily on first strikes against enemy networks.\(^{50}\) In October and November of 2007, the PLA held a weeklong exercise named “Iron Fist-2007” which included testing electromagnetic warfare. In addition to conventional live-fire training drills, the exercise involved implementing advanced cyber warfare, jamming, and spoofing techniques.\(^{51}\) The PRC has already demonstrated its ability to penetrate a variety of protected computer systems and potentially use computer network and electronic attacks to strike U.S. civilian and military infrastructures.\(^{52}\) The term *shashoujian* (commonly translated as Assassin’s Mace) is an increasingly frequent – although ambiguous – reference in Chinese military writings. It resembles asymmetric weapons in that it is used to level the playing field between two unequal opponents, but it differs in that it is a single decisive weapon for completely crippling an enemy.\(^{53}\) While there is no definitive answer to what *shashoujian* refers to, some believe that a highly advanced cyber warfare infrastructure appropriately fits the


\(^{49}\) The Heritage Foundation, *Trojan Dragon*, 2-3.


\(^{51}\) Minnick, “China Conducts Electromagnetic Exercise.”

\(^{52}\) Wang and Stamper, “Asymmetric War?” 173.

definition as it could provide the power to incapacitate a state’s electricity grid, transportation systems, and communications array.\textsuperscript{54} The idea is particularly appealing since many Chinese use a Linux OS instead of a Microsoft one, potentially shielding them from the larger effects of wide-scale cyber warfare.\textsuperscript{55}

For many, information warfare of this scale may still seem appropriate to a fantasy world, or at least one not in the near future. However, China has developed its asymmetric power in conventional dimensions as well. Along with its expansion of IW infrastructure, the PRC has invested heavily in ballistic and cruise missiles, as well as undersea warfare systems (including submarines and advanced naval mines).\textsuperscript{56} One of the most well-known capabilities is its anti-satellite weaponry, which China employed to destroy one of its own aging weather satellites in January 2007.\textsuperscript{57} In modernizing its air force, the PLA has highlighted the greater need for attack craft over bombers, stressing the importance of aerial precision-strike power for deterrence, protection, and assault.\textsuperscript{58} China has a large arsenal of various platform-based missiles, including land based DF-21 (CSS-5) medium-range ballistic missiles for potentially hitting aircraft carriers. Even in 1996, when the PLA was still a newly-professionalized organization trying to find its own feet, military leaders were procuring weapons for a potential asymmetric conflict such as a Russian destroyer armed with eight nuclear-capable Sunburn missiles, one of the most lethal anti-ship cruise missiles.\textsuperscript{59}

\textsuperscript{54} Fritz, “How China will Use Cyber Warfare to Leapfrog in Military Competitiveness,” 64-66.
\textsuperscript{55} Thornton, \textit{Asymmetric Warfare}, 64.
The PLA’s focus on anti-ship weaponry reflects their understanding of how much global power projection depends on aircraft carriers. By studying the recent wars in the Balkans and the Persian Gulf, the Chinese are finding ways to adapt to America’s reliance on naval projection via carrier groups. They have started moving their fiber-optic communication systems underground and their defense facilities away from the coast, into western China and out of naval missile range. In building up a correlative offensive capacity, the navy (PLAN) is increasing its holdings of over a dozen types of anti-ship cruise missiles, including subsonic and supersonic rocket-powered missiles such as the SY-2 and FL-7.

Based on the increasing reliance of the PLA on modern applications of information technology and its desire to expand its asymmetric power, investment in C4ISR and IT lie at the center of China’s strategy for modernization. While IW is a critical element in the overall Chinese military doctrine of warfighting, their conception of asymmetric warfare goes beyond this. The PLA has never renounced the use of physical means in a future conflict with the United States or any other opponent, believing it will rely primarily on conventional forces once a strategy of deterrence fails. In a showdown with Taiwan, many ranking leaders see air power and defense against air strikes as “hold[ing] the key to victory or defeat.” But this does not mean that asymmetric warfare can be dismissed. The PLA will be able to employ their air power, not to mention their naval power, under asymmetric strategies. Moreover, they will be able to supplement this with various forms of information warfare.

62 C4ISR is a holistic doctrine of command, control, communications, computers, surveillance, and intelligence.
63 Lewis and Xue, Imagined Enemies, 241.
The Reality of the Threat

The issue in need of examination now is whether China’s development of asymmetric power is likely to be a considerable danger in the future. Certain asymmetric approaches seem inconsequential compared to the death and destruction of conventional war. However, they should not be made light of. The importance of China’s asymmetric power is not that it will turn the current global power distribution on its head through bloody world wars. Asymmetric power will give the PRC a vital edge in winning the smaller and restrained conflicts it is most likely to fight. There is no question that China is lagging behind the United States in terms of military and information technology.64 The United States will not simply stand still as China modernizes. It is unrealistic to assume that the PRC will be able to easily catch up and surpass America in the fields the latter currently excels at. But asymmetric power will allow the PLA to dish out a tough serving in any small-scale war where Beijing has limited political aims. The authors of Unrestricted Warfare, although often exaggerating the advantage that China will have in the future, presciently identify the application of “unlimited measures” to a set of limited objectives.65

Nowhere is this more evident than in China’s biggest flashpoint, Taiwan. For the PRC, victory in any conflict over Taiwan essentially means attaining particular goals quickly enough to achieve an irreversible outcome. The greatest emphasis on asymmetric warfare capabilities has been related to contingency planning over Taiwan.66 Not only does Taiwan have a relatively low level of information and computer security, while being highly dependent on IT, but it also has an unexpectedly low readiness level for a direct conventional attack – especially compared to

---

64 Paarlberg, “Knowledge as Power,” 134-137.
65 Qiao and Wang, Unrestricted Warfare, 210-211.
other states under national security threats such as Israel or South Korea. Moreover, the PRC could use information operations like CNO and electronic attacks, as well as cruise missile strikes against aircraft carriers, to delay U.S. military intervention long enough to achieve a set of limited military and political objectives. The fact that the United States’ military is superior overall to China is irrelevant in the types of conflicts most likeable to bring these two combatants together. Such conflicts would pit the bulk of China’s power against only a fraction of America’s – owing to U.S. commitments elsewhere in the world.

Past evidence and studies suggest that seizing the initiative is embedded in the Chinese military doctrine as a “preferred course of action.” The Chinese have displayed this preference in their military actions during the Korean War; conflicts over the offshore islands, especially Jinmen; the multiple crises in the Taiwan Strait; the border wars with India in 1962 and the Soviet Union in 1969; and the attack on Vietnam in 1979. Together, initiative and asymmetry form a potent combination drastically multiplying the likelihood of Beijing achieving its objectives in local conflicts. China’s asymmetric capabilities will pose a major problem in the Taiwan theater if the PLA can "deter, delay, deflect, and, if necessary, defeat the United States" in any restricted conflict.

Furthermore, while a fight over Taiwan is the most probable, it is not the only potential conflict that could erupt. From 1988-1999, the PRC was involved in 9 out of 13 military clashes

70 Ibid., 106-120.
in the South China Sea.\textsuperscript{72} These armed confrontations mainly involved Vietnam and the Philippines but also Taiwan and Malaysia. Many of these conflicts were over the Spratly Islands which six states have claimed. In 1995, the Philippines accused the Chinese of building a permanent military installation on Mischief Reef. Beijing denied such accusations and refused to withdraw. Although China has pledged to resolve the dispute peacefully, the Philippines’ military relations with the U.S. (specifically the Mutual Defense Treaty of 1951) make this another potential flashpoint in the future.\textsuperscript{73} The PRC could also find itself in a shooting war with India if it presses ahead with the Yarlung Zangbo Hydroelectric Project, which would divert the waters of the Indian Brahmaputra River to supplement power the Three Gorges Dam provides.\textsuperscript{74}

Asymmetric power would enable China to achieve a victory in any of these limited conflicts. However, there are some who believe that too great a focus on irregular combat is dangerous because it would ultimately come at the expense of what American military power is most well-known and regarded for, high-intensity conventional war.\textsuperscript{75} They see this emerging consensus that the challenges of the twenty-first century will come mainly from unconventional and asymmetrical threats as unwarranted. In this argument, irregular warfare is not unimportant, but it should be treated under the categories of counterinsurgency and state-building, as distinct from military capabilities, because generally the causes of irregular warfare are those other than military aggression.\textsuperscript{76}

This is a valid and important point about the military’s role regarding counterinsurgency and state-building. However, the argument inappropriately confines asymmetric warfare to these

\textsuperscript{73} Ibid., 125-126.
\textsuperscript{75} Michael J. Mazarr, “The Folly of ‘Asymmetric War,’” \textit{The Washington Quarterly} 31, no. 3 (Summer 2008): 46.
\textsuperscript{76} Ibid., 35-38.
categories. Asymmetric warfare can be applied by state actors in a variety of ways that are detrimental to the United States in conventional combat. These methods are not just those that terrorist groups employ but any strategy designed to force a strong power into a situation where it is “unable to make use of the power it has.” Anti-ship cruise missiles are an effective asymmetric counter to the power projection capabilities offered by aircraft carriers. Imagine a cyber attack that alters the numerical figures on the computer screen of a military logistician. How would people know what to trust? In responding to a crisis in the Taiwan Strait, what if an electronic attack disables the transportation of American supplies and personnel, preventing them from effectively participating in the island’s defense? Such a case is a perfect illustration of how asymmetric power could help the PLA delay American intervention long enough to achieve its particular aims.

Conclusion and Policy Implications

In bracing for potential future conflicts with China, the shadow of asymmetric warfare looms large. However, fears that the Chinese will use asymmetric approaches such as cyber warfare to completely undermine America’s power and defeat U.S. hegemony are exaggerations. Although the PRC may someday surpass the United States as a global superpower, it will not be because of asymmetric warfare. The real threat of asymmetric warfare is not that it will propel China to challenge the global power distribution, but that it will provide a significant advantage to the PRC in winning conflicts with limited stakes and scale.

The United States will need to balance itself on a fine line between completely restructuring its military towards combating asymmetric threats and concerning itself only with traditional capabilities. Recent indications suggest that the United States is overhauling its forces

---

77 Qiao and Wang, *Unrestricted Warfare*, 212.
for fighting irregular war.\textsuperscript{78} While this is itself a good sign, there is a danger that policy makers will go too far in this shift. It is imperative that the U.S. maintains its lead in conventional warfighting because great power war is far more destructive than asymmetric war. From a military standpoint, greater defense against cyber attacks is practical for preventing the setbacks the PLA would be hoping to cause in any conflict where the Chinese would be sure to lose force-on-force. However, if the U.S. allows its traditional capabilities to slide far enough that other powers could feasibly challenge it on the conventional battlefield, great power war may reemerge as a frequent threat to international security.

As with any situation involving limited resources, moving the military towards specializing in asymmetric warfare will involve some trade-offs with its capacity for major conventional warfare. Military commanders and defense planners will continue to be at the forefront of this shift, but contributions can also come from outside these groups. Better legal definitions and moral clarifications would be very helpful (e.g. establishing a morally and legally appropriate response to an electronic attack that disables an area’s power grid and leads to hundreds of deaths). It is important to take the time to figure out and make clear whether or not the U.S. would be justified in responding to a Chinese cyber strike with traditional force.

The risk of great power war means that any shift towards greater efforts to combat asymmetric challenges must be done carefully and realistically. Nevertheless, such a shift is necessary if the United States wishes to prevent China from significantly expanding its power through coercion. It is also worth noting that developments in combating asymmetric threats do not necessarily detract from conventional capabilities. The two types of warfare are sometimes compatible; improvements in one area can benefit the other. A greater asymmetric deterrence

capacity would not only help nullify the PRC’s advantages in a limited conflict, but may reduce the likelihood of such conflict occurring, since Beijing would have lower chances of attaining its particular goals. The necessity for such a shift to occur seems, in light of China’s growing asymmetric power, a matter of strategic logic.
Bibliography


Romberg, Alan D. “Future East Asian Security Architecture: Implications for the PLA.” In Swaine et al., 311-335.


T’ai Kung. “Six Secret Teachings.” In Sawyer and Sawyer, 40-105.


