CHINESE NATIONAL STRATEGY OF TOTAL WAR

GRADUATE RESEARCH PAPER

Michael J. Good, Major, USA

AFIT/ICW/ENG/08-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/ICW/ENG/08-02

CHINESE NATIONAL STRATEGY OF TOTAL WAR

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Warfare

Michael J. Good, BA

Major, USA

June 2008

AFIT/ICW/ENG/08-02

CHINESE NATIONAL STRATEGY OF TOTAL WAR

Michael J. Good, BA

Major, USA

Approved:

_____/signed/_____ _____

Robert F. Mills, PhD, USAF (Chairman) Date

_____/signed/_____ _____

Dennis D. Strouble, PhD, USAF (Member) Date

Abstract

The purpose of this research is to examine the recent trends in the growth of China's national power across all elements to determine if there is an underlying national strategy based on the Chinese concept of total warfare. This research seeks to determine if China is currently engaged in a total war with the United States across nontraditional forms of conflict including economic, political, information, financial, cyber, and industrial warfare.

This research was performed by literature review of Chinese military theory and Chinese government policies supporting China's efforts to modernize its military and economy through technological advancement. The results of this research indicates that China does possess a long term national strategy for engagement in a total war with the United States consistent with Chinese military strategy, and is actively pursuing this strategy across all elements of national power.

To my wife and son for the love, support, and understanding
they provided throughout this year

Acknowledgements

I would like to express my sincere appreciation to all those that helped make my year at AFIT a successful and memorable experience. I wish to extend my sincere thanks to Dr. Robert Mills who allowed me into the Cyber Warfare, my fellow students in the Cyber Warfare IDE program who have been great friends and mentors, and my fellow Army brethren who have helped keep me grounded in both professional and personal development.

Michael J. Good

Table of Contents

AFIT/ICW/ENG/08-02

CHINESE NATIONAL STRATEGY OF TOTAL WAR

I. Background

The purpose of this research project is to examine the concept that China is currently engaged in a long term cyber conflict with the United States and other technologically advanced nations across the full range of national power consistent with Chinese cultural and philosophical concept of "Total War".

The genesis for this research originated with an initiative from the Office of the Secretary of Defense to leverage Joint Professional Military Education institutions to look at long term strategic facing the United States. The original scope of this research was to examine the way the People's Liberation Army would incorporate civilian economic capabilities and infrastructure to support cyber warfare operations. After engaging in research however it became apparent that the scope was based on three significantly faulty assumptions. First was the assumption that there is a significant distinction between the civilian and military economic infrastructure in China similar to that of the United States, something this research will attempt to demonstrate is probably not valid. Second was the assumption that the political and economic infrastructure would be used to support the operations of the PLA which would provide the direction and purpose for utilizing the cyber capabilities. This research questions the premise of this assumption postulating that instead the PLA is in fact supporting the political and economic elements of national power by providing organizational and operational

support consistent with the requirements for national defense and the national strategy as established by the Chinese national leadership. The final assumption is that the civilian economy and infrastructure is intended to be used as part of a Chinese military response to military conflict with the United States. While this assumption is a valid in the event of conflict, research indicates the Chinese are already using cyber capabilities within their economy and infrastructure in a manner consistent with Chinese military strategy and doctrine without any indication that armed conflict between China and the United States is currently imminent or even likely.

After determining the original assumptions were invalid the scope of this research was restructured to examine the current Chinese doctrine, policies, and activities in cyber space to determine if they are consistent with the Chinese principles of warfare. The research is intended to answer the specific question, "Are the Chinese cyber capabilities actively being used in a manner consistent with the military principles to undermine the capacity and will to engage in military conflict with China?" To answer that question this research focused on Chinese military, cultural, and economic philosophy from the traditional sources of greatest influence to current policies and doctrine being implemented in china today. The research will also examine the relationships of the elements of national power in China specifically the relationship within the military and the economy. The research will also examine the Chinese employment of cyber capabilities across the spectrum of national power consistent with these philosophies.

II. Total War

Chinese doctrine centers on the concept of total warfare which is the total application of national power across the full spectrum of diplomatic, infrastructure, military and economic elements to destroy an enemy's will or its capacity to wage war. The doctrine of Total Warfare is not the same as Unrestricted Warfare in that the Chinese do not engage in military operations against civilian targets in an asymmetrical use of force but rather compete with adversaries within their element. It is also not the same as unconventional warfare since the purpose of the total warfare doctrine is not to engage military forces specifically against psychological centers of gravity but to use the full spectrum of national power to achieve this goal. Although the Chinese total warfare doctrine does stress destroying an enemy's will to fight it also reduces the capacity of an enemy to engage in warfare. And finally total warfare is not the same as asymmetrical warfare although any of the elements of national power can be applied asymmetrically across the spectrum to any of enemy's elements of national power.

The Chinese concept of total warfare is not new and can be found as far back as the writings of Sun Tzu and other military philosophers of the early Chinese era. This concept of total warfare is also used by iconic leaders Mao Tse Tung and Deng Xiaoping. The philosophy of total warfare was incorporated into Mao's concept of guerrilla warfare and the People's Revolution, in Deng's 24 Strategies, and in the writings of senior military academics which serve as guidelines for many of the current philosophies of the Chinese leadership. One of the best examples of the methodology of this philosophy was produced by two senior PLA Air Force Colonels, Qiao Liang and Wang Xiangsui, who wrote a monograph titled "Unrestricted Warfare" which outlines a model for using high

technology and economics to defeat a superior adversary without engaging in military conflicts (US Embassy, 2001). This model is reflected in the current doctrine of People's Revolution in the information age. Although this philosophy is not new the current pace of technological advancement especially across the cyber domain and the use of cyberspace have made the model not only possible but have made it practical in a time efficient matter. To gain a better understanding of his total warfare doctrine we will look at these four major philosophies which currently shape Chinese strategic planning.

Sun Tzu

The Chinese military philosopher Sun Tzu is probably the most widely quoted and studied military strategist of the modern age. Although the seminal work by Sun Tzu is entitled “The Art of War” some argue this is more properly translated as “The Art of Conflict” (Griffith, 1963: ii). Sun Tzu looked at military operations not simply as a conflict between armies but as a conflict between nations characterized by the elements of national power. Sun Tzu readily understood that to defeat any enemy one must either destroy the enemy's will to fight or their capacity to fight but that this destruction did not have to take place on the battlefield or even as a result of military engagements. Sun Tzu's philosophy on conflict stresses the concept that an enemy ultimately could be beaten without any fighting at all with the proper application of strategy to defeat an enemy while disguising any hostile activities. They key to defeating an enemy’s will is to understand what motivates them and what is the source of their strength. By attacking the enemy where he is weak you could undermine his confidence and defeat his will to fight.

Another key concept of Sun Tzu's philosophy is that understanding yourself and your opponent is the true key to determining the outcome of any conflict. Without a correct understanding of what your opponent's objectives, capabilities, and motivations are, it is difficult to devise a strategy to defeat them. Therefore good leaders attempt to disguise or deceive their opponent on their own objectives capabilities and motivations. Good leaders are also honest and objective in evaluating their own strengths and weaknesses.

Another key element of Sun Tzu's philosophy was the economic cost of conducting warfare. Pivotal to this philosophy was the ability to use the enemy's resources against them so that his economy becomes weaker while yours becomes stronger until they are no longer capable of sustaining conflict. Another element of this economic principle was the ability to capture a conquered enemy intact when possible so that the conqueror would gain the benefit of this resource rather than have to rebuild it. Sun Tzu also advocated the strategy of using others to fight your battles leaving them to bear the cost of the conflict, or taking advantage of misfortunes which would drain the resources of an opponent leaving him vulnerable to attack.

Sun Tzu placed a very high value on spies and the information they provided. He stated anyone who fails to get information from spies because he is unwilling to pay the cost of them is devoid of humanity (Griffith, 1963:144). The information gathered by spies was crucial to gaining an accurate understanding of the enemy and the situation so that the correct strategies could be employed. Sun Tzu divided the spies into five categories: the native spy, inside agents, double agents, expendable agents and living spies based on the rolls and information they could provide. Native spies and inside

agents come from the enemy's populations and political leaders; they provide information on the enemy intentions. Double agents and expendable agents carry misinformation to the enemy to deceive him about our own intentions. Living spies are those who returned information about enemy activities. The interaction of these five types of spies is what Sun Tzu referred to as the "Divine Skein" (Griffith, 1963:145). The foresight gained from spies was not only crucial in determining the strategy of when and where to strike the enemy but was also an essential element of psychological warfare both in motivating your own people and in defeating the will of an enemy.

Mao Tse Tung

No man in modern Chinese history has had a greater influence than the great leader himself, Mao Tse Tung. Mao was a military commander of the Red Army during the Revolution between the Communists and the Nationalists led by Generalissimo Chang Kai-shek. During the period of communist revolution they were also engaged in warfare with the Japanese army and often fought alongside pro-nationalist forces against the greater enemy. Mao was an astute student of the classics of Chinese warfare stratagems and was an avid reader of Sun Tzu. Mao also understood that battles were just a small part of the overall war, and its results were often determined by the characteristics which led him to the battle. Mao understood that the Red Army was not in a position to fight either the Nationalists or the Japanese without developing a strategy that would allow them to build strength over time while weakening his opponents. As a result Mao developed a strategy of People's War in order to strengthen the Red Army and to win the support of the Chinese people who would not overtly with engage in conflict,

but would provide support, sustenance, and the intelligence the Red Army would need for the long war.

It was this development of the People's War and the effective use of propaganda that enabled Mao to continue fighting and which induced many of the Nationalists to join his cause. Mao's strategy was so effective that whole units of the Nationalist Army deserted and joined the Red Army bringing all of their equipment and greatly enhancing the capabilities of the Red Army. In accordance with the stratagems articulated by Sun Tzu about capturing enemy units intact Mao's strategy was to welcome these deserters into the Red Army and treat them as trusted soldiers. As a result Mao not only gained personnel already trained in military tactics but they became fiercely loyal to his cause. Mao also gained modern war fighting equipment causing him to famously remark them in a 1930s letter to his subordinate commanders "we have a claim on the output of the arsenals of London as well as Hanyang and what is more, it is delivered to us by the enemy's own transport corps. This is the sober truth and not a joke (Tung, 1936)".

Even more important than the equipment and personnel was the intelligence he received from the multiple types of spies especially the former Nationalists whom Mao treated with great kindness and respect, allowing him to conduct a defensive war. With this information he avoided the enemy strengths, and engagements with superior forces, while instead striking where the enemy was weak or exposed. This stratagem of People's War was so successful that after Mao had defeated the Nationalist Army, Mao renamed the Red Army the People's Liberation Army and initiated universal conscription as a way to indoctrinate and build support for the Communist Party. He also

began the use of propaganda and Information Warfare which has been expanded upon by the Communist Party as a current stratagem for building national unity.

In addition to being a student of the classics, Mao was also an innovative commander who understood the nature of long-term warfare. Mao wrote two seminal works which outlined his campaign strategy to his military commanders entitled On the Protracted War and Guerrilla War. These two works described the tactics a weak force uses against a strong due to the support of the people, allowing the Red Army to acquire resources by trading land for time and by undermining the source of enemy strengths as applied to China in the 1930s. Mao understood that battles need to be shaped and that conditions for success could be developed by bold commanders using the intelligence provided by the Chinese people. Mao also believed that outside of battle, the military's effort should be to support the people in developing the resources they would need to sustain themselves over a long war and that during times of battle, all available resources should be used to support the military including civilian infrastructure and organizations such as hospitals and police forces (Tung, 1936).

After the defeat of the Nationalist forces Mao became head of the Communist Party and the leader of modern China. Most of the senior leadership of the Communist Party (and of the nation) held positions in the Red Army during the communist revolution. It is therefore unsurprising that many of the tactics used by the Communists to defeat the Nationalists and the Japanese would be instituted by the new government into the civil and political structures, including building and maintaining support, using propaganda and Information Warfare, and interoperability between the military and civilian infrastructures.

Deng Xiaoping

Outside of Mao Tse Tung the most influential leader in modern China was Deng Xiaoping. Although his only official government position was Chairman of the Communist Party's Central Military Commission, Deng Xiaoping's influence was such that many consider him the de facto leader of China after Mao's death. Deng Xiaoping was the architect of the reforms leading to China's current modernization efforts and the development of the national strategy of “socialism with Chinese characteristics.” The outline of this national strategy was set forth in Deng Xiaoping's 24 stratagems which detailed how China would use technology and industrialization to catapult it into a leading national power but would do so in a way that avoided direct conflict by not drawing attention to China’s growing strength. His modernization effort centered on reforms in four pillars of Chinese society: agriculture, industry, science and technology, and the military. His objective was to restructure the inefficient state-run industries in a manner that would allow them propel China's economic rise by allowing capitalism with Chinese characteristics.

One of the key factors in the success of these modernizations was in the emphasis of pragmatic solutions over Marxist principles which had proven so destructive to the Chinese economic system. As part of his reforms, Deng Xiaoping applied the same principles of the weak versus strong used by Mao and Sun Tzu, however Deng Xiaoping expanded them not only to cover military affairs but to all elements of national power, understanding that China was not strong enough to defeat the leading industrialized nations in a military conflict but would have to engage the nations in other forms of conflict such as economic warfare, information warfare, and even political warfare. The

backbone of this new national strategy was to build a Chinese manufacturing capability to take advantage of their large population and low labor costs. This in turn would allow China to leapfrog into high-tech industries through indigenous research and development and leveraging foreign technology. All of this would allow China to rapidly catch up with more advanced industrialized nations. It would also allow China to restructure their military-industrial complex to support civilian production making them cost efficient, and better able to modernize their military forces. By building up their manufacturing capacity, China would be able to support its own indigenous industries while preventing the foreign industries from being able to capitalize on China's growing middle class. In addition there is increased emphasis on education especially in high technology areas where China seeks to replace the need for foreign technology transfers, thereby decreasing any potential economic gains that would be made by foreign companies.

21st Century Strategy

In 2006, China announced a new national strategy in the People's War which recognizes the effects of technology its role in future warfare (IOSC, 2006). This new strategy entitled the People's War in the Information Age represents a direct evolution in the concept of total warfare. Although the strategy was produced for the PLA is a military strategy, it is still consistent with the goals and objectives outlined by the Communist Party and the Chinese leadership to strengthen Chinese national power across all elements. This new doctrine is described in many of China's leading policy institutions. The highly influential National Defense University theorizes that technology is removing the distinction between military and civilian organizations, especially in

areas such as dual use technology, which play an important part in economic, organizational, and information exchange innovations.

Under this new strategy the Chinese also recognize that the key to winning future conflicts will not be thru high technology weapons alone, but thru the combination of advanced weapons and low cost technologies used in creative and innovative ways (Ryou, 2008). The strategy also recognizes that future warfare will not have well defined battlefields, but will be fought globally and may not be fought between nation states. Instead conflict will be among nation states and other organizations using low-cost tactics which take advantage of this explosion in technology.

Another shift it postulates is a changing form of combat to a method less about killing power and more about psychological influence which is why future battlefields will include places such as the media, the stock market, and computer networks where the potential exists for a very small group of people to have a tremendous impact for a relatively low cost (US Embassy, 2001). As a result of the changing battlefield conditions, China is seeking to develop new types of soldiers capable of operating in this new environment. These new soldiers are far different from traditional soldiers and may not even serve in the military at all. They include people like computer hackers to conduct cyber warfare operations, academics who study science and economics, business leaders who can adapt to organizational changes and human innovation and can apply the principles of strategy across all elements of national power to these new battlefields.

Another fundamental element of this new strategy is recognition that control of the flow of information is crucial to success on the new battlefield. This control of information extends beyond the ability to influence the enemy but the ability to influence

internal elements to support national policies. This approach would mean that organizations such as the Ministry of Public Security which monitor the Chinese computer networks through the Golden Shield project are just as important as the PLA in this new age of warfare. This new information age battlefield includes almost any aspect that touches the daily lives of the average person and is further reducing the distinction between military and civilian domains.

III. The Conduct of Total War

In the previous chapter we outlined the doctrine of total warfare and how it has developed over the 6000 year history of Chinese military strategy. Now it is essential to look at the infrastructure and policies which support this doctrine of total warfare. This infrastructure goes far beyond the traditional military organization to include the political, economic, social, and educational organizations that conduct operations in the new battlefields of the information age. This new infrastructure includes the Ministry of Public Security and the "Great Firewall of China", as the "Golden Shield" project is commonly called, which controls the flow of information across the Internet which serves as both a security device and as a propaganda device in a time when the news media is increasingly digitized in the 24-hour news cycle. The Ministry of Public Information also controls a large part of the information content that flows, into, inside, or out of China through control of the Chinese telecommunications and media outlets. This includes everything from telephones, television, and radio allowing the government to control what people do and do not see.

On the political and economic battlefields China's Ministry of Trade and Foreign Ministry are just as important to the total war as the Defense Ministry. Through the use of international organizations like the United Nations, the World Trade Organization, and others, China is able to shape global opinion, conduct economic warfare, and influence policies that will help them achieve their national objectives. These ministries also control access to the 1.2 billion Chinese consumers and wield significant economic power in support of the national policies to gain technology and foreign capital to modernize the Chinese economy. Even the education system in China serves to support

the national strategy through the use of technology, with emphasis on science and mathematics, and its partnerships with foreign corporations that support the transfer of technology. All of these actions help to prepare the Chinese to fight across the multitude of battlefields needed to support a total war strategy.

Even within the PLA most of the focus remains on its modernization effort to develop new capabilities, especially in the domains of space and cyberspace. Most people remain completely unaware of the economic structure of the PLA and the fact it controls a multitude of corporations, research and development centers, and universities which are a large part of the Chinese economy. The PLA research and academic institutions continue to define the future strategies for the conduct of future warfare that seeks to downplay armed conflict in favor of less destructive forms of conflict in nontraditional battlefields.

Ministry of Public Security

The Ministry of Public Security is the Chinese national police force. The MPS is like a conglomeration of the US Federal Bureau of Investigations (FBI), the US Border Patrol, Immigration and Naturalization Service (INS), and Department of Homeland Security (DHS). Although it is responsible primarily for the civilian criminal law enforcement and does not traditionally engage in paramilitary operations, the People's Armed Police, a branch of the MPS has a paramilitary function similar to the US Coast Guard during times of military conflict. There are approximately 300,000 people serving in the Ministry of Public Security performing functions which continue to support the national strategy of total warfare in a variety of ways. As previously mentioned, the MPS is responsible for the “Golden Shield” project which is an Internet monitoring and

security program. The Golden Shield project serves as an effective front line of defense against cyber attack providing thousands of trained personnel who would help defend Chinese network infrastructure. It also serves as an effective tool for information and economic warfare as well. It is yet another example of dual use technology that gives China the capability to conduct cyber warfare but whose obvious military applications are simply considered a sidebar of its civilian function.

The technology for creating a Golden Shield project is another example of technology transfer which has greatly increased China's capabilities across a spectrum of total warfare. Through a combination of technology and self-censorship China has the ability to not only control the flow of traffic over their network systems, but has the ability to scan information going over those networks looking for key words or phrases. Much of the technology for the Golden Shield project was purchased from American companies, such as Cisco, which develop and produce routers and intrusion detection equipment. Cisco maintains that the routers were not specifically modified in any way from their other commercial systems, but as a result of the deal they were required to transfer proprietary software code to the MPS. The software that enables the MPS to search for key words is a modified version of this proprietary software (Breaking, 2004). Use of this software has enhanced the ability of the Chinese government to control the flow of information and to crack down on subversives within their society. This not only includes criminals such as hackers, software pirates and porn dealers but other organizations China views as subversive such as religious organizations, pro-democracy groups, and foreign nationals who violate Chinese policies restricting the flow of information (Breaking, 2004).

In addition to their efforts to control the Internet the MPS has been very effective at getting search engine providers, such as Google and Yahoo, to self sensor information and content available to the Chinese people (Google, 2004). China has obtained the proprietary source code, in the name of security, for these popular search engines to enable more effective control over the Chinese networks. This has dangerous implications for other countries since the source code for these search engines and the intrusion detection systems in the Cisco routers is the same as that used by millions of computers in United States and other advanced countries. This could allow identification of vulnerabilities in the software which can be exploited.

The MPS does far more than just monitoring of the network with the Golden Shield project. Every cyber café and Internet hot spot has a monitoring system which tracks every individual user that enters or passes through the system. All users are required to present some form of official identification before logging on in public Internet sites that all public computers are strictly monitored.

Monitoring the national network is just one of the many things that the MPS does to support the national strategy. As a national police force, they are responsible for immigration and for monitoring foreign visitors and the purpose of those visits. Activities of foreign visitors are often monitored, and there are widespread allegations of telephone call monitoring, individuals being followed, and electronic eavesdropping at locations frequented by foreigners. Foreign visitors whose activities do not conform to the Chinese policies especially in religious activities or human rights advocacy result in harassment and/or deportation.

The Ministry of Education

The Ministry of Education seems an unlikely spot for the conduct of total warfare, but it stands at the foreground of the transformation of China by producing large quantities of well educated students prepared to handle the rapid pace of technological innovation needed to carry out the strategy of total warfare. The contributions of the education system to the total warfare strategy are many and varied from education to indoctrination. The Chinese place in exceptionally strong emphasis on the math and science skills needed to support technologically advanced industries. In international competitions, Chinese students routinely place near the top in both of these categories across all educational levels. Chinese universities graduate more engineering students each year than nearly the entire European Union combined, including computer science majors (Martin, 2005). In addition to its own domestic education programs the Ministry funds the education of thousands of Chinese nationals at universities in foreign countries where they make up a significantly large portion of the students in the technologically advanced fields such as computer science, engineering, and mathematics. The US remains the top destination of Chinese students, and it is estimated that more than 100,000 Chinese students are enrolled in US universities, more than half of them in graduate or research programs. The Ministry also takes advantage of technical innovation such as computerized classrooms, telecommunications, and distance learning to increase the level of education in rural areas of the country increasing the pool of educated workers available for high tech industries. Chinese universities are routinely partnered with foreign companies as a result of Chinese trade policies, creating in an influx of technological innovation to which these universities can study and exploit for the benefit

of Chinese indigenous industries. This will allow them to compete directly with partner corporations seeking to unlock China's vast untapped markets for high-tech goods and services. The Chinese Academy of Science alone has over 500 virtual enterprises in the high-tech sector.

The Ministry of Trade

China has experienced tremendous economic growth since the start of its open door policy in 1978. The Ministry of Trade controls the access to the 1.2 billion Chinese which gives it a tremendous amount of economic and political power. China's regulations regarding domestic and foreign investment is heavily slanted in favor of domestic production and their trade policies are some of the most discriminatory regarding the rights and obligations of foreign partners. The US Department of Commerce receives numerous complaints of unfair Chinese trade practices, but most companies are afraid to complain too loudly for fear of losing access to the Chinese markets. China’s coercive trade policies prevent any foreign corporation from owning significant interest in Chinese companies and are heavily restrictive in favor of indigenous manufacturing. Numerous tariff and non-tariff trade barriers exist that restrict foreign investments and make selling foreign-made products directly to China's 1.2 billion consumers a difficult, if not impossible, prospect. China explicitly defines what types of foreign investment is prohibited, permitted, or encouraged, with the latter category focusing on advanced technologies. Foreign investors in high-tech industries enjoy preferential treatment in the such as tax rebates and lower tariff rates as an incentive to transfer technology but at the same time are subject to regulations not imposed on domestic competitors (McCormack, 2006). Any high technology firm doing business in China is forced to accept the Chinese

policies requiring the transfer of technology. This frequently includes explicit provisions for technology transfers in the forms of local content requirements, production and export photos, and/or collaboration in production and research or training. Contracts with foreign companies impose conditions designed to ensure technology transfer, while joint ventures with foreign partners involve technology sharing and seek to promote development of next-generation technologies in China.

An increasingly frequent type of commercial offset requires that foreign technology firms enter into agreements to establish training or research centers that would allow the Chinese access to developing technologies while increasing their own domestic capabilities to compete in domestic and foreign marketplaces. By creating these research centers, China is moving beyond the realm of imitation in manufacturing and technology and establishing the prerequisites for creative innovation. Currently what technological advances exist are disproportionally due to foreign investment capital and technology rather than indigenous technical advances.

With the backing of the Chinese government, these training and research centers may soon prove capable of absorbing the technology, skills and processes needed to move ahead of their foreign partners (BEA, 2006: ii - iv). Even more importantly the technology from these centers is being applied to other sectors of the Chinese industrial base making them more competitive, especially in the realm of electronics and aviation. This would indicate that in the long term Chinese trade balances with foreign nations would continue to progressively increase in favor of China as Chinese exports in high technology industries advances to become competitive globally. As a result of China's discriminatory policies, most US companies currently engaged in collaborative research

risk losing monetary and technical gains from their investments as Chinese trade policies continue to support China's export centered economy. Despite China's restrictive investment policies, requirements for technological transfer and indigenous production, many companies are willing to accept the risks associated with doing business in China and are even more willing to exchange cutting edge technology in order to gain a foothold in the Chinese marketplace. Fear that a competitor could gain access to the Chinese market first has caused some companies to accept conditions that will virtually eliminate any long term benefits (BEA, 2006: 44-47). This competition for access is used by China as a method of enticing competitors to ensure the continued flow of investments and technology to help build and maintain the Chinese high technology industries.

Technological transfers are not the only way in which the Ministry of Trade supports the total war strategy. China's trade policies regarding tariffs and enforcement of trade agreements are highly selective reflecting the national strategy to expand the Chinese national power. The Chinese trade policy places restrictive tariffs on foreign goods that compete against domestic products and uses "Free Trade" zones and "High Technology Development" zones to steer foreign direct investment to underdeveloped areas of the country. This saves Chinese billions of dollars by getting foreign investors share the costs of building the electrical and telecommunication infrastructure required to support these manufacturing facilities.

Even where foreign investors have been successful in establishing entrance into the Chinese market selling foreign manufactured goods in China is still commercially unviable. Chinese policies require the establishment of joint manufacturing ventures for foreign companies seeking to sell products in China. These joint ventures prevent foreign

companies from selling their products directly to the Chinese by controlling distribution channels, mandatory export quotas that keep products out of the Chinese market, and product content requirements that prevent foreign manufactured goods from entering the Chinese market (BAE, 2006: ii – iii). In addition to keeping foreign goods from directly competing with domestic product, weak enforcement of property rights also keep foreign goods out. This cost foreign companies an estimated $500 billion a year. Piracy in the software and entertainment industries is estimated as high as 90%, and enforcement efforts by Chinese officials are ineffective in stopping it. Chinese industrial policies require that foreign firms conform with state industrial policies that require complex approval processes that force companies to submit very detailed and even proprietary or confidential information including technical specifications, manufacturing processes, designs, blueprints, formulas, or patents (BAE, 2006: 45-47). According to Underwriters Laboratories (UL) this certification process is extremely costly to foreign companies in the form of lost time, travel expenses for Chinese inspectors, and multiple approvals from numerous government agencies. Products that do not receive certification cannot be imported, exported, or sold in China (Dubinski, 1997). In addition to the cost of getting the certification the cost to foreign companies must include the cost from increased completion that imitates the manufacturing processes to produce competing products without the associated costs.

The Chinese Foreign Ministry

The Ministry of Trade is not the only ministry that uses economic power to support the total war strategy. The Chinese Foreign Ministry plays a pivotal role in economic policies through negotiation of trade agreements and by representing China's

interests in international economic forums. The Foreign Ministry has been successful in influencing policies that give China significant advantages in international trade and finance. As with technology, the prospect of gaining an economic foothold in China has resulted detrimental long term trade policies by China's major trading partners. These policies will likely result in growing trade deficits. An example of these policies is US granting Most Favored Nation status (MFN) to China despite concerns about trade laws, environmental conditions, human rights abuses, substandard conditions for workers, and failure to meet its obligations under existing trade agreements.

One successful example of the Foreign Ministry influencing economic policies has been getting China designated as a developing country by the World Trade Organization (WTO) despite an economy that places them above many of the developed nations. This designation allows China to employ the strategy of total war in economic and financial domains while exempt from many of the policy requirements faced by China's competitors. China uses this designation to delay complying with policies on trade tariffs, enforcement of trade agreements, and access to domestic markets. One of the most significant exemptions for China has been protection of its defense industrial base under provisions of the WTO (Weiping, 2000:1). This exemption prevents Chinese defense industries controlled by the PLA from having to comply with WTO trade practices, despite competing with civilian companies. These companies produce hundreds of nonmilitary and dual use products for the civilian market at distinct advantage over competitors. The Foreign Ministry has great success in using the WTO and other international forums to file costly time consuming grievances against countries that seek to force China to adhere to requirements opening its markets (Weiping, 2000:7). China's

Foreign Ministry has also been highly effective at using bilateral and regional agreements to reduce the influence and prestige of competing nations in Asia. China has the second largest foreign reserves in the world behind Japan, and the Foreign Ministry uses this financial tool to negotiate favorable trade policies with less developed, resource rich, nations in Asia. China also invests in these less developed markets giving China new markets for their exports.

While active in the economic domain, the Foreign Ministry is the primary conduit for projecting Chinese political power supporting the total war strategy. Through use of diplomacy the Foreign Ministry enables China to pursue the total war strategy without attracting much attention. The Foreign Ministry has been successful in deferring attention away from China by supporting high profile regimes such as Iran, North Korea, and Venezuela which receive considerably more international focus because of their adversarial diplomacy. These governments maintain hostile relations with the US allowing China to gain considerable prestige serving as a mediator for international agreements, such as the six nation framework with North Korea, while maintaining the perception of impartiality. This enables China to gain significant trading advantages through preferential trade negotiations in exchange for diplomatic support.

In diplomatic forums such as the UN, China wages continuous propaganda warfare to shape perceptions and deflect attention from issues such as human rights, environmental protection, and unfair trade policies. Publicly China presents a friendly face and supports the policies that give it the greatest political advantage, behind the scenes China often is accused of undermining policies not in their national interests rendering them ineffective.

The Foreign Ministry does not just serve as the face of China abroad but its eyes and ears as well. Every diplomatic official serves as a conduit for intelligence collection activities. Intelligence gathered through overt sources in the Foreign Ministry allows China to develop effective strategies to influence international opinion. Numerous reports suggest that China also uses the Foreign Ministry to reach out to ethnic Chinese communities in an effort to engage in intelligence collection activities in highly technical fields like nuclear weapons, computers, aerospace, and electronics.

The People's Liberation Army

When most people discuss the PLA they focus on the traditional military subjects assessing it in terms of capabilities, equipment, force size, training levels, soldier's morale, and the ability to project force. This assessment is usually specific to how the military will conduct operations on some future battlefield. While these issues are valid, they are only a part of the complex issues that must be examined to understand the nature of the PLA and its contributions to the strategy of total warfare. One thing that must be understood is that the PLA is not just a military force for national defense, but a significant part of the Chinese political, economic, and social structure. Historically the PLA embodies the communist revolution, and was the mechanism which enabled the communists to defeat both the Japanese and Nationalist Forces. The PLA serves as the mechanism which communist leaders have used to maintained control of the nation during periods of internal strife. The PLA's origins can be traced to the early days of the communist revolution when it was commanded by Mao Tse Tung. Nearly all of the early leadership of the Communist Party served in the PLA during the years of guerilla warfare through the post WWII era. These leaders studied military tactics and strategy as well as

communist philosophy. With Mao's ascension as head of the Communist Party many of his senior military commanders and key subordinates were placed into party leadership displacing leaders loyal to the Nationalist government. They also displaced senior leaders of the Communist Party who did not support Mao or his policies. During this period of turmoil Mao's uncontested grip on the military allowed him to impose his will on the new government. Recognizing the importance of keeping the military loyal and to keep the populace under control Mao renamed the Red Army the PLA and instituted a policy of universal conscription. This ensured that everyone would be forced to go through military training and indoctrination under the watchful eyes of political officers. Universal conscription provides a common bond between most of the male population and serves as an entrance point into the Communist Party. Since Mao, no President or Premier has been selected who did not have military service and who did not head one of the several military commissions in the Politburo which control the PLA. This fact demonstrates the power of the PLA within the Chinese government, and that these leaders have all been trained in the principles of Chinese military strategy which they apply to other elements of national power. They are also cognizant of the long term nature of strategy and develop plans that may take decades to achieve, but which are carried out with a unity of purpose since the change in political leadership does not directly affect the long term national strategy.

The PLA of modern China is not just a political indoctrination organ for the state. It is rapidly transforming into a modern, well equipped military force beyond what is required for simple national defense and capable of projecting Chinese power regionally to secure vital national interests. Over the last five years spending on the PLA has topped

16% of the national budget (Mederios and others, 2005: xviii). The PLA has started production on seven new types of naval ships and submarines including an antiaircraft platform similar to the US Aegis class cruiser, two new classes of domestic jet aircraft, upgraded missile systems and amphibious capabilities. Nearly all of this was made possible through the acquisition of technology from foreign sources. China claims these weapons are defensive in nature designed specifically to protect the sea routes use to transports the economic resources, including oil, which must travel through chokepoints in the Indian and Pacific Oceans that could easily be threatened. This seems unlikely considering the countries bordering those choke points are not hostile to China and are not seen as potential adversaries from a military standpoint. These chokepoints however border countries that are economic competitors including India and Indonesia, as well as pass through the territorial waters disputed by China and several neighboring countries. These nations all lay claim to the various small islands like the Spratly Islands which are believed to sit above petroleum deposits that would belong to the island's owners. Given this situation it seems far more likely the PLA is engaged in an attempt to intimidate nations that attempt to claim these islands by demonstrating the ability to defend them.

The PLA modernization is not limited to equipment, but includes reform to its personnel system and the organization structure of the PLA itself. China has spent a tremendous amount of effort studying how technology has changed the way wars are fought, specifically from the post Gulf War period, to determine why high tech armies are better at war fighting than numerically superior but less advanced countries. Spurred by the continuing push from leading defense research tanks and universities, China is transforming the way it views future warfare and the types of soldiers required to fight

them. Universal conscription has long meant massive numbers of recruits that perform their obligatory service and leave the military. This situation common to conscript armies means that most soldiers never progress beyond the basic set of fighting skills. Most of the true capability and training resides in the officer corps which is better educated and trained. In more technologically advanced militaries this situation is nearly the opposite where most capabilities are provided by a well developed professional cadre of enlisted soldiers who are trained to be proficient in the use of technology and creative innovations. China is restructuring the PLA to create active units of professional soldiers that can meet the immediate defense needs, the ones with the most modern equipment, and is moving many low technology man power intensive areas from active duty to the People's Reserves. One report even suggests that China might end universal conscription for the active component and make it a reserve function saving billions of dollars that could be used to increase the rate of modernization and for training the professional forces (IOSC, 2006).

Another key item is the professional development of the military through training and exchange programs with allied nations. This gives China an opportunity to increase its military and political influence with other nations in the region, often reducing the influence of countries outside the region such as the United States and Russia. By conducting these training exercises and exchanges the Chinese are able to spread their military doctrine, find potential customers for their military equipment, gain valuable insight as to the military capabilities in the region, and demonstrate the PLA's capabilities to potential adversaries.

The Chinese military has also put a great deal of thought into what future battlefields might look like and is seeking to develop new units and recruit new types of soldiers to fight in areas not traditionally considered battlefields. Chinese military theorists cite the single greatest factor influencing the decline in military power is failure to develop the right units to fight future fights rather than units that could fight past conflicts better (US Embassy, 2001). Chinese military theorists believe that traditional armed conflicts between nation states are unlikely, and future conflicts will be fought through economics, information, political influence and technology. Future battles are likely to be fought in space and cyberspace instead of traditional domains. Future battles are also likely to trend away from killing power to precision strikes designed to cripple an opponent or render their weapons systems ineffective allowing them to be controlled without killing the crew.

Technology continues to blur the distinction between military and civilian infrastructure especially in the fields of communications where military and civilian communications channels both flow through the same infrastructure making them legitimate targets. To operate in these environments the Chinese military is increasingly looking for technologically savvy recruits from the digital generation who are comfortable operating across the internet as they are flying an airplane or on a naval ship. Future battles will also require soldiers who think in unconventional ways and are capable of integrating low tech solutions that enable them to overcome any technological advantages the opponents might have.

China has long considered the national defense science, technology, and industry to be the foundation of China's economic and technological power and important pillars

in the comprehensive national power. Deng Xiaoping once said “Whether it was in the past, at present, or in the future, China is determined to develop its own high technology and to occupy a position in the domain of high technology in the world” (Henggao, 1994). With its emphasis on technology and industry no other sector of the Chinese economy is better situated to take advantage of technology transfers gained as a result of Chinese trade policies with foreign corporations. Chinese military departments and enterprises make full use of their superiority in equipment, technology, and talented personnel to develop and integrate new technology, which to a certain degree has filled gaps in the civilian fields of science and technology, and raised the overall level of the national economy (Henggao, 1994). The PLA industries are leaders in integrating new technological research. The PLA has benefitted by changing outdated ineffective organizational structures and operational processes to make them more efficient and cost effective (Bitzinger, 2005). In many cases these changes, along with technological advances from foreign direct investment, have helped the PLA generate profits and become more competitive in the civilian market place. It has also increased the quality and competitiveness of the Chinese arms industry.

Unlike the United States, the industrial base of the PLA cannot be separated from the military function that it supports. In the US, the military-industrial complex is separated from the military, and is made up of privately run corporations not directly answerable to the military or government. The PLA is not just part of the military industrial complex in China, but a large part of the economic infrastructure of China as a whole, producing countless items for sale in the commercial marketplace. Within the PLA you can find a number of corporate entities, manufacturing firms and research

centers which are run or controlled entirely by the military, yet produce the computers, telephones, TV sets and other products found within the average home. A classic example of this would be the Commission on Science Technology and Industry for National Defense or COSTIND which is a multinational corporation that runs everything from manufacturing centers and separate think tanks for research and development to universities and multiple corporations producing electronics, telecommunications, testing equipment, and robotics. What makes COSTIND different from corporations in the United States military industrial complex is that the chief executive officer of COSTIND is a senior officer from the PLA. In fact it is entirely possible to become a general officer in the PLA serving entirely in logistics and management positions within one of these corporations and never serving with troops.

COSTIND is just one example of a typical PLA Corporation that serves as the parent for a conglomeration of companies, think tanks, and manufacturing facilities which are able to use the cheap supply of conscript labor, and the military administrative structure to produce goods, many of which have dual uses. As late as the early 1990s it was estimated that PLA owned corporations contributed as much as 90% of the high technology consumer goods to the Chinese economy. It is currently estimated that this amount has shrunk down to about 50% to 60% during the current decade, but is predicted to reach as high as 75% to 80% by the year 2020 with the increased industrialization of China's economy (Blasko, 2001). With a significant portion of the Chinese advanced technology resources and manufacturing capabilities the PLA stands to increase its military budgets as it continues to produce these goods for sale not only in China but worldwide.

Since most factories or industries cannot exist entirely on military contracts or by producing items exclusive for military use this diversification makes sense from a strategic standpoint. It enables these corporations to utilize excess capacity allowing a continued buildup of their military strength. Part of the organized reform in the PLA industrial sector is designed to reorganize these corporations to make them more competitive on the global markets, and to make them financially self sufficient (Blasko, 2001). In 2003 the Chinese military industries as a sector experienced a net profit for the first time as a result of these reforms, and the strength of Chinese exports in these companies. While many companies failed to meet this goal leading sectors such as electronics, and especially the avionics industry have been successful in taking advantages of reforms and benefits such as the exemptions China enjoys from the WTO in order to make a transition to the civilian market.

A great example of Chinese success in using foreign trade agreements to strengthen their military industrial complex through civilian commercial agreements is China's Aviation Industry Corporation (AVIC) (Minnick, 2007). AVIC was formed by restructuring the old Chinese military aviation sector to create a parent company for a group of subsidiaries that are officially listed as civilian companies eligible for foreign investments. These companies have entered into foreign trade agreements which transfer technology directly to subsidiaries that manufacture aircraft for the PLA. AVIC is divided into two divisions AVIC I and AVIC II. AVIC I employs more than 240,000 employees, many of them former PLA soldiers who worked in the old PLA aviation industry, and produces a complete range combat aircraft for the PLA. AVIC I controls 47 manufacturing facilities, 31 research and development centers, and 22 specialized

companies. AVIC II, which is more commercially oriented, controls 78 industrial enterprises and produces over 5,500 aircraft, 700 helicopters, and 10,000 tactical missiles, but the primary outputs of its subsidiaries are the engines, avionics, and other aircraft parts. Each year AVIC exports hundreds of millions of dollars in commercial and civil airplane parts to every major aircraft producer worldwide including Airbus, BAE Systems, Boeing, and DeHavillard. In 2004 Boeing established contracts with four AVIC subsidiaries, worth, $500 million, to produce many of the parts for the Boeing 787 due to enter service in 2008, which means these companies can expect continued financial contracts through the expected 20 year service life of the model.

The benefits of these contracts extend beyond the avionics area. They include spinoff industries like electronics, metallurgy and even the corporate cultures and business practices such as “six sigma” management and quality control techniques that are applied directly to the production of Chinese military aircraft. The impact of technology transfers is a direct threat to the long term viability of foreign commercial aviation companies in China as the PLA continues to come closer to its stated goal of becoming an innovator and producer of high technology weapons and aircraft. Boeing estimates that China will buy 2,600 airliners worth over $213 billion dollars over the next two decades, however as the PLA continues to improve its aviation industry continues to benefit from technology transfers. Past trade practices indicate that China will favor the creation of an indigenous aircraft industry preventing foreign companies from effectively competing in the Chinese market. The economic impacts of this would be felt globally if China went from an importer of commercial aircraft to a global producer especially in countries like the US and France where the manufacturing base for avionics has

significantly declined as a result of outsourcing to countries like China with lower labor costs.

IV. Cyber Space in the Total War

The previous chapters explored the Chinese concept of total war and attempted to demonstrate this concept has been incorporated across all elements of national power into a national strategy supported by the infrastructure and policies of the Chinese government. This chapter will examine the role that cyberspace and the associated elements of cyber power are being integrated across economic and information domains to support directly or indirectly the national strategy of total warfare. In examining this process it should be pointed out that the definition of cyberspace for the purpose of this research is "Cyber space is a domain characterized by the use of electronics or the electromagnetic spectrum and the associated infrastructure for the purpose of collecting, storing, transmitting, or modifying data" (DoD, 2006). It should also be pointed out that although the preceding chapters focused primarily on China as a nation state many non-state actors also participate in the total war concept with varying degrees of overt or tacit support by the Chinese government. These non-state actors include corporations like Lenovo computers or Huawei Telecommunications at one end of the spectrum, which are ostensibly civilian companies independent of the Chinese government's direct control, though as will be examined later both have strong ties to the government and access to senior Chinese political and military leaders. The other end of the spectrum includes software pirates, identity thieves, and hacker groups like the Honker Union, which officially declared cyber war against the United States. Despite the criminal status of these organizations and activities there is little effort on the part of the Chinese government to crack down on these activities and there is credible evidence to suggest that the Chinese government encourages these activities privately while lamenting them

publically. Between these two extremes lies a diverse mixture of industrial sectors, media outlets, research and development centers and social organizations competing across the cyber domain. The collection of government organizations and non-state actors have differing goals and objectives such as Information Warfare, cyber spying and economic warfare, but whatever the objective there can be little doubt that China is actively engaged in the cyber domain.

Cyber Spies

Sun Tzu postulated that five different types of spies should be used by the good general to gain the foreknowledge needed for victory. Today the cyber spy is revolutionizing the way information can be obtained from open sources to the most closely guarded secrets. Cyber space allows almost anyone with network access and average computer skills to become a cyber spy, capable of searching for information across the spectrum of national power. Cyber space offers significant advantages over traditional intelligence methods including the fact that identification and attribution of these activities are exceptionally difficult to prove to the level required for legal action. In April 2006, before a meeting between German and Chinese heads of state, it was revealed that the German government network had been penetrated and the email accounts of top German officials including the Chancellor's had been compromised (Lemos, 2008). The German government publically accused China of conducting the operation, and the Chancellor spoke about it directly with Chinese Premier Wen Jiabao during the week long summit (Marquard and Arnoldy, 2007:1-4). The accusations by Germany joins a growing chorus from other nations including the US, France, Great Britain, Japan, and India over the last two years, yet despite the accusations nothing akin to a 'smoking gun'

has been publically released demonstrating China's culpability for the attacks (Walker, 2008). Officially the Chinese government denies any involvement in cyber attacks against foreign governments and calls the accusation irresponsible. The Chinese government points out that Chinese law forbids any form of cyber crime that undermine network security and that Chinese law enforcement agencies are willing to work with the law enforcement agencies from other countries to investigate these crimes (Peter, 2007).

The enforcement of cyber crimes in China is however somewhat selective. It is estimated that over 25,000 people in china have been jailed for cyber crimes which violated China's internet restrictions over the last five years, but there has not been a single known case of a Chinese citizen arrested for conducting cyber crimes against a foreign government. Chinese cyber spies are not just interested in government information but commercial information as well. The cost of cyber crime against US corporations alone is estimated to be billions of dollars a year from viruses, loss of proprietary information, and recovery costs. Exact figures are impossible to acquire because many companies are fearful of the impact of reporting cyber crimes, and the cost of the damage from these attacks is hard to measure (CSR, 2004: 12-14). The sophistication of the attacks is of a level that most routine security measures do not even detect the intrusions indicating that these attacks are more than the random acts of individual or even groups of hackers, but are being conducted by the Chinese military or other state run organizations (Walker, 2008).

The ability to penetrate security systems without detection is one of the major things that make cyber spies far more valuable than tradition spies. Since victims are unaware they have been penetrated they continue to assume their security systems are

working allowing the attacker continued access. Internal security measures within a network are often much easier to overcome which means once a system is penetrated that system becomes an agent working for the spy to gain inside information. While it is usually difficult, costly, and time consuming to develop inside spies scanning a network for vulnerabilities can be much faster and with less risk of discovery.

Cyber space is more than computer networks, and cyber spies have been operating across the whole of the cyber domain. Communications technologies are a logic target for the cyber spies especially in the era of cellular telephones and satellite communications. Cyber spies are constantly using high technology means to intercept this flow of communication. Despite the security of encryption and other security measures numerous methods exists to target these communications as they pass through parts of the infrastructure where information is less protected.

China's Telecommunications Industry

China's telecommunications industry is dominated by four major corporations Huawei, Datang, Zhongxing, and Julong, which appear to be independent private sector actors unrelated to the government ministries governing the telecommunications industry. This illusion is quickly shattered by examining the origins and partnerships of these corporations. Huawei the largest and best known of the four is a perfect example. Like the others Huawei was formed as a civilian offshoot of the military in 1988 by Ren Zhengfei, the former director of the PLA General Staff Depertment's Information Engineering Academy which is responsible for all telecommunications research for the Chinese military including command and control systems warfare (Mederios and others, 2005:218-220). Huawei maintains deep ties with the Chinese military which remains one

of Huawei's largest customers and sponsors 44% of the research and development as joint research projects. Huawei is one of the world's top ten producers of telecommunications equipment and since its entrance into the export market it has expanded into a global wide corporation with offices in 45 countries. Huawei started by rapidly penetrating into Africa, Russia, India and many other countries especially in southern Asia, not served by western telecommunications companies (Mederios and others, 2005:220).

Huawei has also benefitted from political clout which almost no other telecommunications company enjoys. When Huawei attempted to purchase a major subsidiary in India the Indian Ministry of Defense sought to prevent the sale citing the sale could compromise the Indian military communications systems and repeated and persistent cyber attacks from China. When the purchase was expected to be rejected by the Indian government Chinese President Jiang Zemin personally contacted the Indian Prime Minister about the sale which subsequently was approved (Gilley, 2001).

Huawei's close ties to the government are closely mirrored in its ties to the military. Despite the fact sales and services to the Chinese military comprise only 1% of total sales the PLA is the largest research partner, and has significantly benefitted from the transfer of technology acquired through Hauwei's extensive partnerships with US and other foreign companies. Hauwei's domination of the telecommunications market in many of the poorer and developing countries in Africa and Asia, and its close ties to the Chinese government demonstrate the ways in which the Chinese government's national power can be enhanced without attracting the scrutiny of the international community. This fully supports the strategy of total war by disguising the danger represented to the

command, control, and communications infrastructure of the countries where Huawei does business. Another example of the unrecognized danger this represent is Hauwei's attempt to buy in partnership with Bain Capital, a British investment firm, a significant stake in the 3Com Corporation, an American electronics firm that deals in telecommunications automation especially in the field of communications encryption and intrusion detection (McCotter, 2007). The 3COM encryption system and intrusion detection software are the standard for nearly all of the communications systems and computers for the entire United States Government, including the Command and Control systems for the US military. By acquiring a stake in 3Com, Huawei would have had access to the proprietary software used to defend a majority of the computers and telecom systems in the United States.

Chinese Manufacturing and Industrial Sector

The Chinese industrial sector is by no means a monolithic block operating at the explicit orders of the Chinese government but they serve as an effective element in expanding China's national power through cyber space. With its huge labor pool, less restrictive regulations on labor policies and lack of environmental protections, China has become a manufacturing powerhouse. A vast multitude of industries have turned to partnerships with Chinese manufacturing firms to replace expensive manufacturing plants in their home countries with low cost imports from China. Not only has this caused a weakening of the manufacturing base of these countries, but it has brought a multitude of benefits to the Chinese firms that have enabled the successful transfer of technology and business practices. These technology transfers have in turn enabled the development of the technology China needs to support its total war strategy. The danger does not have to

come from any deliberate efforts to undermine the economies of the targets, but result from the fact that the loss of manufacturing capacity has left many countries dependent on a nation whose national interests may not align with their own.

Lenovo Computers is a perfect example of the way Chinese manufacturing supports the strategy in cyber space. Like Huawei, Lenovo is a spinoff of the military and produces computers, software and other electronics. Lenovo is currently the largest manufacturer of computer chips in the world and its products are not just used in computers but other electronics devises ranging from cars to automated teller machines. As a result of this Lenovo is involved in over 500 foreign commercial partnerships which not only bring in new technology through these joint ventures but which represents a potential method by which the Chinese can influence global markets.

One example of the dangers this represents is the computer industry. In the US every major computer manufacturer, Dell, Gateway, IBM, Apple, and HP have transferred production of their computer chips and mother boards to China. This means that there is the possibility any computer bought from these companies could be designed with a multitude of potential security risks that could be exploited under the right circumstances. Many concerns have been raised about this potential threat, and these companies have policies to test the supply of products against these possibilities, but even the most stringent tests may not be enough to ensure the risk does not exist (Tkacik, 2007:19).

Even if this activity were discovered there is little that could immediately be done to fix the problem because the US lacks the domestic manufacturing capability to replace the infected computers or the chips. Even without software concerns the possible danger

exists that quality control issues or manufacturing designs could result in vulnerabilities that could be exploited to shut down the systems. Design defects such as a vulnerability to power surges could have catastrophic effects. Computers and communications devices that use satellites to connect to the internet could be built with internal vulnerabilities that would allow them to be attacked through the wireless systems. Although there are no indicators that these activities have taken place or that the Chinese have a deliberate strategy to do so, as long as countries remain dependent on Chinese manufacturing for electronic goods the possibility this could be exploited continues to exist and would be consistent with the Chinese strategy.

Hackers and Other Cyber Criminals

Chinese hackers are some of the most practiced and prolific cyber hackers operating today. Over the last five years you cannot pick up a business paper, IT journal, or computer magazine without finding some reference to hacking activities that have been traced back to China. While most Chinese hackers prefer to operate in obscurity, some Chinese hacking groups make dramatic gestures, such as the declaration of war against the United States by the Honkers Union, specifically to draw attention to them to increase their reputations. Although it is extremely difficult to prove these hackers are endorsed or supported by the Chinese government, the attacks are so deliberate, sophisticated, and well organized it is hard to believe it is not government directed.

The US Department of Defense (DoD) is by far the most popular target for Chinese hackers. Other branches of the US Government including the Commerce, Homeland Security, Justice, and Energy Departments also make the top ten list of Chinese targets (Reid, 2007). Chinese hackers have been responsible for high profile

attacks such as the 2003 Titan Rain attack against the Pentagon, the 2006 attack which infected and shut down the network at the Naval War College, the 2005 attack on the British Defense Ministry, and the penetration of the networks of the German Chancellor. These high profile attacks are just the tip of the iceberg. These attacks make the news because they were designed to be discovered since the overt intent was to impede the networks of these organizations. It is not known if the overt activity served as a cover for more covert operations.

A vast majority of the Chinese hacking activities are not designed to affect the networks they penetrate but are designed to retrieve data. Research centers and think tanks are constantly barraged by attacks including the most secure facilities in the United States like Sandia National Laboratories, Oak Ridge National Laboratories, and Jet Propulsion Labs. The attack on the Oak Ridge Labs was so sophisticated it penetrated the defenses and was able to receive more information in one day than Chinese scientist Wen Ho Lee was able to sneak out of Sandia National Labs over several years (Kesselman, 2008). Chinese hackers also commonly target nongovernmental computers in sensitive industries relating to commerce, academia, industry, finance and energy with a wide variety of attacks ranging from spear phishing, malicious websites, viruses and denial of service attacks to the penetration of networks for the purposes of stealing research and conducting industrial espionage (Rogin, 2007). While many of these attacks are crude brute force attacks common to “script kiddies” a significant portion demonstrate the same precision and sophistication that indicate an organized effort more commonly found in military units than the loosely organized collection of hacker groups.

More indicative of Chinese government involvement than the targets is the sheer volume of these attacks and the number of people that would be required to carry them off. China has some of the most restrictive internet policies and the most sophisticated network monitoring programs of any country in the world. For the Chinese government to deny they are involved is an open admission that the “Golden Shield” project and the draconian measures to control the network are ineffective; however this would be inconsistent with the facts. China has an estimated 25,000 citizens a year who are arrested and fined for hacking activities designed to avoid network monitoring by the Chinese government and gain access to religious, political and other sites outlawed by the Chinese government. Some human rights groups and IT related organizations go so far as to suggest that in order to avoid prosecution these hackers are forced to put their cyber skills to work for the Chinese Government targeting foreign governments and business interests. This tactic, they say gives the government plausible deniability, and if they are forced to take action they can point directly to these acknowledge cyber criminals (Breaking, 2004).

Besides hackers Chinese cyber criminals, acting alone or with the encouragement and support of the government, cost US and other corporations billions of dollars in lost revenue. Piracy in the computer software industry is rampant and enables Chinese computer companies to avoid paying licensing fees for proprietary software allowing them to sell to the domestic market much cheaper than foreign competitors. Industrial espionage is increasingly becoming high tech and there can be little doubt that the Chinese government has benefitted from these activities. In 2006 the British Rolls Royce company was attacked with a virus that downloaded terabytes of data to unknown servers

in mainland China. Months later that same material was discovered on computers at a joint research project between the PLA and a US aviation company (Tkacik, 2007).

The entertainment industry is another big area where cyber crime has cost the US economy not just in the Chinese market but worldwide as these products are marketed to other countries. The quality of the products and the ease with which the pirates manage to export the products, despite the multitude of Chinese government agencies that are in charge of international trade and transportation, indicate either the government is enabling the efforts, or doing little to try and stop them.

PLA Cyber Warfare

The PLA is considered by many to be at the forefront of the planning and integration of cyber warfare. Chinese military scholars have put a great deal of research into identifying the role cyber space will play in future conflicts and China has become universally acknowledged as the leading cyber threat. Chinese military academia has produced a litany of research about the potential of cyber space as a battleground in future wars that could be used to attack not only military targets, but could be used against financial, industrial, and infrastructure targets in the civilian sector which have dual use capabilities or are essential to the conduct of modern military operations like satellites and telecommunication. The research also examines the effects of economic warfare targeting banks, financial markets and other targets of great psychological value. Nearly all of the research centers on how China could defeat a technologically advanced nation, usually the United States, by denying them use of the technology they depend on. The Chinese have also been the leaders in identifying the tactics and the types of soldiers which would be capable of fighting in cyber space and in the creation of weapons that

would enable them defeat the enemy through cyber power. Chinese strategic planning for cyber warfare has been going on for more than a decade and during that time Chinese strategists have developed a number of plans and scenarios to use cyber power to attack an enemy through information warfare and electronic means. The principal fundamentals of these strategies rely on early penetration of the enemy cyber infrastructure, usually prior to the advent of hostilities, and then the elimination of these capabilities at the crucial moment to cause the psychological defeat of the opponent (Spencer, 2008). To support this strategy the China has created military units designed to conduct cyber operations in electronic warfare, computer network operations and information operations (Thomas, 2001:2). According to the US Defense Department the Chinese military began creating information warfare units in the PLA and Peoples Reserves in early 2000 but the existence of these units is denied by the Chinese government which called them baseless attacks against China reflective of the cold war mentality of a bygone era. These cyber warfare units have already been attributed with penetration attacks on US military networks where they conduct intelligence collection and reconnaissance on US strategic plans and capabilities (Tkacik, 2007).

A majority of these units are being created in the People's Reserves and are based around the technology rich coastal regions. The recruits for these units are primarily the younger generation of university students from the numerous science and technology universities that are found in these provinces. The PLA also holds annual hacking competitions as a way of identifying potential recruits who become subcontractors to the military conducting hacking operations for the PLA while allowing plausible deniability. The winner of the first competition, who uses the cyber name Wicked Rose, created a

consulting company which went to work for a PLA managed IT company and was identified as responsible for several attempts to penetrate into a research and development network at Lockheed Martin a US defense firm (Reid, 2007). The use of such unorthodox recruiting methods by the PLA underscore the belief that the role of the traditional soldier is under transformation where recruits are selected based on their intellectual agility and likely will be able to fight future wars without ever having to exit their front door.

To effectively utilize these new cyber units the PLA has created a number of strategic battle plans that can be applied against opponents. The cyber attack on the Baltic country of Estonia is a good example of the power of cyber attacks to cripple a nation without the need for military force and demonstrates how cyber attacks could be used against civilian targets. Chinese strategists have studied United States training and doctrine and have created a virtual guidebook for how to conduct cyber warfare against the US (Price, 2007). The US and other advanced nations use technology as force multipliers to enable missions to be accomplished with fewer soldiers. The Chinese playbook calls for disrupting these force multipliers through cyber space leaving the forces inadequate for their mission forcing them to withdrawal. An attack plan based on this strategy produced by two PLA Air force Colonels, Sun Yiming and Yang Liping, was used in a recent military exercise to demonstrate that they could cripple a US aircraft carrier battle group through cyber power and prevent it from being able to conduct operations in support of Taiwan (Reid, 2007).

Another lesson from the Estonia incident the Chinese have plans to exploit is the widespread vulnerability of modern society. After analysis of the attack on Estonia, a cyber defense expert at the Pentagon testified before the US Congress that a cyber attack

on the scale of the one in Estonia could leave 70% of the US without power for six months. Attacks on communications infrastructure and satellites could be devastating, and the psychological impact could be equivalent to that of a weapon of mass destruction. China's anti-satellite capabilities could be used early in a conflict to eliminate GPS and intelligence gathering satellites. China is also actively researching ways to blind these satellites electronically without having to destroy them.

Chinese cyber units are reportedly also working of a whole range of other tools such as botnets, viruses, and backdoor programs that could be used to attack communications networks and allow the Chinese access to strategic and operational plans. As a result of Microsoft's business ventures in China it is a near certainty that the Chinese cyber units have access to the source code for the Microsoft Office suite used on nearly every computer in the United States including the US government which gives them a virtual skeleton key for accessing millions of computers (Tkacik, 2007:16). The Chinese cyber units are preparing for the full range of Information Warfare operations in cyber space and this includes information operations (IO), military deception, and psychological operations (PsyOp). The Chinese routinely incorporate these operations into their plans and exercises (Thomas, 2001:2-3). The Chinese constantly seek to shape international opinion in favor of China and continue to advocate the idea that China's military modernization is needed for defensive purposes. Government officials maintain that China does not possess any cyber units despite the fact that their military academia has been developing tactics and strategies for how those forces would be used in future wars.

Another area the Chinese IO has been successful is maintaining the focus on military conflict over Taiwan. With cross straight activity as the focus the PLA has shown the US and other governments exactly what they have expected to see in terms of a traditional military conflict and the associated modernization of Chinese forces. This myopic view routinely ignores the fact that China's military is increasingly designed towards less lethal methods such as cyber operations that can be used immediately and without warning to overwhelm an opponent and prevent a military response. The development of these capabilities gives China significant political influence in the region as many countries fear they could be the targets of these cyber attacks. It also ignores the fact that China's industrial sector is extremely dependent on foreign resources including oil which China requires in greater supply. With resource rich islands in the South Pacific under dispute and vast untapped resources just north of China in sparsely populated areas of Russia it is far more likely that China will engage in military conflict to gain favorable access to these resources than a military conflict to impose its will on Taiwan.

V. Conclusions

The analysis of the research indicates that the Chinese government is engaged in a national strategy to become a major global power by the year 2050. This national strategy extends across all elements of national power and is being conducted both symmetrically and asymmetrically between elements. The Chinese military academics have been theorizing about the nature of future conflicts in the information age and have been prolific in writing about the types of soldiers, weapons, and tactics that will be need to fight across the expected battlefields over the next generation. From a historical stand point China's total warfare strategy is consistent with Chinese strategic philosophy extending back for over 6,000 years.

The Chinese government consistently attempts to deny the existence of any grand strategy to engage in total warfare, but an analysis of the work by leading Chinese intuitions and think tanks when compared to the activities of Chinese government and non-state entities show a high degree of correlation beyond what could be explained by coincidence. The coordination and synchronization of Chinese economic, political, and industrial activities bear a striking resemblance to the tactics and strategies that Chinese academics and theorists believe would be employed in future conflicts. Chinese policies on economics, education, commerce, industry and foreign relations all work together to expand China's national power.

Chinese military modernization and expansion far exceed its stated purposes of national defense (Tkacik, 2007:19). Given the lack of any projected threat to China over the foreseeable future, and the development of new information warfare units designed to engage in operations across the cyber space domain, indications are that the Chinese

government is pursuing an objective beyond those claims. Given the accumulated data it is fairly certain that the Chinese are engaging in activities to defeat the United States and other nations through nontraditional forms of warfare without engaging in open hostilities.

Despite the fact that a wealth of indicators point to China's conduct of economic, informational, industrial, and political warfare against the United States there seems to be little recognition by most Americans that they are engaged in a total war with the Chinese. What is even less evident is the fact that the United States is mainly responsible for providing the Chinese with the financial, technological, and political support that is being used against them. Through trade policies that place economic interests ahead of reasoned restraint and the continued transfer of technology to China the United States has greatly enhanced the capabilities and industrial power of China far above what it could have reasonably done on its own.

Trends such as decreased educational performance, the decline of the US industrial capacity, and long term national debt only serve to increase the effectiveness of the Chinese strategy. Chinese strategy also takes advantage of another long term trend the transition of the United States from an industrial to a service based economy. Chinese strategy is designed to undermine the long term viability of the US economy by seeking to develop its own indigenous technological capabilities. Though the use of its economic markets and discriminatory trade policies China has created partnerships and joint ventures with technology leaders that will virtually force those companies to develop next generation technologies in China or risk losing millions of dollars spent trying to gain access to Chinese markets. Based on China's past performance development of this

indigenous technological capability will eliminate any significant long term opportunities for foreign firms to gain access to China's markets. With the development of future technology being conducted in China, US companies will also find increasing competition for a declining poor of workers and college graduates in high technology fields as the Chinese will require increasing numbers of these people to work in its high tech industries.

Cyber warfare plays a significant part within the strategies for these high technology industries. The Chinese have not shown a great indigenous capability for creative thinking in the development of new technologies rather they have shown creative imitation of technologies copied from more technologically advanced countries including the United States. To this end the use of cyber warfare trained troops within the PLA to conduct espionage against US corporations to steal industrial secrets, technological advances, production and manufacturing techniques, and other information that would allow them to modernize their equipment and compete on a global market serve both the military and economic function. As a result of this activity China increases its economic power at the expense of the US while following Sun Tzu's maxim "the wise general sees to it his troops feed off the enemy".

It is estimated that the theft of intellectual property rights in China costs the US economy billions of dollars each year. If a significant fraction of this theft is being done in support of the PLA and its high technology industries then the US economy is being used to buildup Chinese national power, which may be directly contradictory to our own self-interest. The growth of Chinese national power has seen a significant increase in the size and capabilities of the Chinese military at a time when budgetary and operational

pressures are putting a significant strain on our own military as we struggle to modernize or own forces.

Even more alarming is the fact that these technological advancements especially in the fields of communications and electronics could serve as a method to negate the US technological advantage in military equipment. As China enters into corporate agreements with firms like Microsoft, Cisco and 3COM they gain access to the proprietary software that is used by the US military as well as government agencies and US businesses which may enable them to build viruses or other cyber weapons to disrupt the critical infrastructure of the United States to support the Chinese national strategy.

China and the Future

Despite the fact that China has successfully conducted total warfare against the US for more than a decade the situation has not reached a point where the Chinese strategy of total war cannot be countered. China faces a host of significant problems including an aging and disproportionately male population, a ecological problem that is steadily getting worse, a growing middle class that is increasingly capitalistic, ethnic and religious strife, and a youth population that is growing further removed from the history and ideology of communism and Maoism. China's total war has demonstrated great success primarily because it has not been viewed in the same context by the United States and other nations with which China has been engaged. China's government and non-state supporters have had the advantage of a unified strategy while the United States has failed to identify the nature and extent of the threat and form a comprehensive response. If the United States and other targeted countries were to develop a comprehensive plan to combat the Chinese across the full spectrum China could face tremendous difficulties in

achieving its goals. To develop and implement any sort of effective response the United States must first openly acknowledge and articulate the activities of the Chinese government. The US must use all elements of national power to fight back and it must set forth a clear national strategy to protect US interests. The US should strengthen alliances and use international forums to isolate China and to force the end of the discriminatory trade practices that have been supporting China's total war strategy. The longer it takes for the US to muster the national will to engage in this total war with China the less capable we will be to win it.

Bibliography

1. Blasko, Dennis. “Inside the Chinese Defense Industry” Defense Intelligence Reference Series VP-1920-271-90

2. Blitzinger, Richard. “The PRC’s Defense Industry: Reform without Improvement”. *China Brief*, 5:1-4,The Jamestown Foundation. (March, 2005)

3. “Breaking Through the ‘Golden Shield’”. *Garden Networks*. (December, 2004)

4. Bureau of Export Administration (BEA), Office of Strategic Industries and Economic Security. *U.S. Commercial Technology Transfers to the People’s Republic of China*. Defense Market Research Report, Washington: Government Printing Office, 2006

4. Carafano, James and Weitz, Richard. “Combating Enemies Online: State Sponsered and Terrorist Use of the Internet,” *Heritage Foundation Executive Summary Backgrounder*, 2105, (February, 2008).

5. Congressional Research Service (CSR). *The Economic Impact of Cyber Attacks*. Government and Finance Division Report produced by Cashell, Brian, Jackson, William, Jickling, Mark and Webel, Baird. Washington: Library of Congress, 2004

6. Dubinski, Kristin. Certification Scheme of the People’s Republic of China. Underwriters Laboratories Inc. (1997)

7. Gilley, Bruce. “Huawei’s Fixed Line to Bejing,” *Far Eastern Economic Review*, (January, 2001)

8. Griffon, Samuel B. Sun Tzu: The Art of War (translation by the author). New York: Oxford University Press, 1963

9. “Google conforms to Chinese Censorship”. *Newsmax*. (September, 2004)

10. Henggao, Ding as quoted by Pillsbury, Michael. “Reforming Defense Science and Technology, and Industry”. Originally appeared in *China Military Science* (Summer, 1994), reproduced by the Institute for National Strategic Studies (September, 2005)

11. Information Office of the State Council (IOSC). *China’s National Defense in 2006*. People’s Republic of China, 2006

12. Kesselman,Rachel F.“Chinese Cyberwarfare” Intelligence Brief to the International Relations and Security Network Security Watch. Washington DC, 11 January 2008.

13. Lemos, Robert. “U.S. Military Flags China Cyber Threat”. Information Warfare Monitor. (March, 2008)

14. Marquand, Robert and Arnoldy, Ben. “China Emerges as Leader in Cyber Warfare”. *Christian Science Monitor*. (September, 2007)

15. Martin, William., World Bank Representative. “Will Technology Be a Source of Chinese Influence?,” Keynote address to China in Asia Seminar Series, Seminar 3, American Enterprise Institute, National Defense University, 13 May 2005

16. McCormack, David H., Under Secretary US Commerce Department. “Win-Win High Technology Trade with China,” Remarks at the Center for Strategic Studies, Washington DC, 9 June 2006

17. McCotter, Thaddeus G. “Communist Dissonance (Part One): ‘Hauwei and the CFIUS’. *Human Events*. (November, 2007)

18. Medreios, Evan , Cliff, Evan, Crane, Keith, and Mulvenon, James. *A New Direction for China’s Defense Industry: Rand Project Air Force Report.* Contract F49642- 01-C-0003, September 2005

19. Minnick, Wendell. “China’s Defense Industry Benefits From Foreign Commercial Deals”. *Defense News*. (July, 2007)

20. Peter, Tom. “Alleged Chinese Hacker Attack Stir Digital Cold War”. *Christian Science Monitor*. (September, 2007)

21. Price, Michelle, quoting a Pentagon report by Larry Wortzel of the Army War College. “China’s Blueprint for Cyber War”. *Information Age Today*. (11 September 2007)

22. Reid, Tim. “China’s Cyber Army is Preparing to March on America, says Pentagon” *Washington Times*, (8 September, 2007)

23. Rogin, Josh. “Cyber officials: Chinese Hackers Attack Anything and Everything” *Federal Computer Week*. (13 February, 2007)

24. Ryou, Hayoun. “Chinese Cyber War,” Institute for Defense Studies and Analysis Strategic Comments, (22 January 2008)

25. Spencer, Julien. “Pentagon Report Eyes China’s Cyberwarfare, Antisatellite Programs”. *Christian Science Monitor*. (March, 2008)

26. Thomas, Timothy L. “China’s Electronic Strategies,” *Military Review*, 217, (May – Jun 2001).

27. Tkacik, John J. “China’s Quest for a Superpower Military,” *Heritage Foundation Executive Summary Backgrounder*, 2036: 16-19 (May 2007).

28. Tkacik, John J. “China’s International Cyber Warriors,” *Heritage Foundation WebMemo*, 1735. (December, 2007).

29. Tung, Mao Tse., Chairman Chinese Communist Party. “Problems of War and Strategy,” Address to the Sixth Plenary Session of the Sixth Central Committee of the Communist Party, 6 November 1936

30. U.S. Embassy, Bejing China. *Summary translation of “Unrestricted Warfare” by PLA Colonels Qiao Liang and Wang Xiangsui*. Washington: Government Printing Office, 2001.

31. Walker, Richard. “China & West in midst of ‘Cyber War’”. *American Free Press*, 130, (May, 2008)

32. Weiping, Ye. “WTO and China’s Defense Industry (Parts III and IV)”, *Strategy and Management*, 3: 1-7 (2000), Chinese People’s University

33. U.S. Department of Defense (DoD). *The National Military Strategy for Cyberspace Operations.* Washington: Government Printing Office, 2006.

Vita

Major Michael J. Good entered military service in 1989 as an Electronic Warfare Signals Intelligence Analyst (98C). After completion of Initial Entry Training Major Good attended the Defense Language Institute where he studied the Russian language and was subsequently assigned to Military Intelligence units in Augsburg, FRG, Fort Stewart, GA and Kunia, HI. After six years of enlisted service Major Good was selected for the Green to Gold program and received an ROTC scholarship. Major Good graduated from Hawaii Pacific University with Bachelors of Arts degrees in Political Science and History. Major Good was commissioned through The University of Hawaii ROTC program as a Distinguished Military Graduate. Major Good's unit assignments include the 5th Bn, 5th Air Defense Artillery, 3rd Armored Cavalry Regiment, 2nd Armored Cavalry Regiment, I US Corps, and the Training and Doctrine Command, Research and Analysis Center. Major Good commanded the 502nd Military Intelligence Company for 18 months including 10 months in Iraq for Operation Iraqi Freedom. Major Good entered the Cyber Warfare IDE program in May 2007, and upon graduation he will return to Iraq as an advisor to the Iraqi Military.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
19-06-2008	**Master's Thesis**	Jun 2007 – Jun 2008

4. TITLE AND SUBTITLE

Chinese National Strategy of Total War

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Good, Michael J., Major, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ICW/ENG/08-02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research is to examine the recent trends in the growth of China's national power across all elements to determine if there is an underlying national strategy based on the Chinese concept of total warfare. This research seeks to determine if China is currently engaged in a total war with the United States across nontraditional forms of conflict including economic, political, information, financial, cyber, and industrial warfare. This research was performed by literature review of Chinese military theory and Chinese government policies supporting China's efforts to modernize its military and economy through technological advancement. The results of this research indicates that China does possess a long term national strategy for engagement in a total war with the United States consistent with Chinese military strategy, and is actively pursuing this strategy across all elements of national power.

15. SUBJECT TERMS
Chinese Military Strategy, Cyber Warfare, People's Liberation Army, China Trade, China Technology

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Robert F. Mills, PhD (ENG)
U	**U**	**U**	**UU**	66	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4527; e-mail: Robert.Mills@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18