Testimony
Cyber Espionage and the Theft of U.S. Intellectual Property and Technology
Committee on Energy and Commerce
U.S. House of Representatives
July 9, 2013
James A. Lewis, Center for Strategic and International Studies

I thank the Committee for the opportunity to testify on this important subject. The hearing is particularly timely coming as it does at the same time as the Strategic and Economic Dialogue between U.S. and Chinese leaders. I will discuss three issues in my testimony: why China steals intellectual property; what the effects of this are on the U.S. and on China; and steps we can take to remedy this problem.

Chinese officials are concerned that disputes over cybersecurity could become a major problem in the bilateral relationship. They are interested in gauging the extent of U.S. concern and finding ways to assuage it. That said, they appear unwilling, absent significant pressure, to give up the long-running national effort to illicitly acquire technology from Western companies. Chinese economic espionage has moved into cyberspace, is now part of normal business practice, reflects deeper problems with the protection of intellectual property, and is so pervasive that it will take years of sustained effort to bring it under control. While an immediate solution is impossible, there must be evidence of progress to avoid further damage to bilateral relations and to reduce a troubling source of instability in international affairs.

Why China Steals Intellectual Property

The Chinese leaders who succeed Mao Zedong in 1978 knew that his policies had left their country in desperate shape. It was impoverished, technologically backward, and falling further beyond most other countries. In a bold move, they decided to open their previously closed nation to western investment. A key part of this opening was China's intention to acquire western technology by licit and illicit means. This acquisition of technology has been part of China's economic strategy for more than thirty years. The foreign investment that flooded into China when its economy opened presented a tremendous opportunity. Foreign firms entering China were pressed in the approval process to transfer technology through joint ventures, in contract negotiations or licensing agreements, or through investment in research facilities in China.

Interviews with numerous companies identify a consistent pattern of behavior. Companies report that technology transfer concessions are a part of business negotiations in China, to provide an advantage to Chinese firms. Chinese regulations and policies can restrict the ability of a foreign company to make Chinese partners agree to confidentiality agreements to safeguard technology or to restrict sales of derivative products. Western firms complain that regulations skew technology transfers in favor of Chinese firms. Companies cite risk to IP, along with regulatory uncertainty, as the two major obstacles to doing business in China. China has relied on the appeal of its growing market to overcome investor reluctance, but there are signs that foreign firms are reconsidering the risks as Chinese firms try to export their own high-tech products to the rest of the world.

There are four reasons that China seeks to acquire technology by any means possible. First, they have an overwhelming desire to catch up with and to surpass the West. Second, they believe that rapid economic growth is politically essential for the party to maintain its dominance. Third, China has no tradition of protecting intellectual property and thirty years of Maoism only made things worse. Finally, the Chinese fear that they have lost the capability to innovate and must depend on stolen technology. In combination, these motives mean that it will be very difficult to get China to change its behavior.

American companies first thought they could control the risk of the theft of intellectual property in China. Most believe that the damage from espionage is part of the cost of doing business in the world's fastest growing markets, and that American companies can create new technologies faster than their competitors can bring the old ones to market and so minimize any loss. Companies used a variety of techniques that would prevent Chinese competitors from getting access. These include holding back key processes from Chinese employees, allowing access only to lower-end technologies, keeping advanced functions outside China, and monitoring employee activities. These strategies provide some protection, but their chief flaw is that they were designed for a pre-internet world. Leaving essential plans stored on a company computer in the U.S. no longer protects them from theft when that computer is connected to the global internet.

The internet makes espionage easier – something we have all come to appreciate in recent weeks. This includes the theft of intellectual property and trade secrets. To give an example, in the mid 1990s an American aircraft manufacturer had an assembly plant in Shanghai. When the American company put surveillance cameras in the ceiling, they discovered that Chinese agents were coming into the plant every night to take things apart, and photograph and copy machinery and plans. The internet provides a new avenue for illicit acquisition. In a more recent case, Chinese hackers simply downloaded blueprints by hacking into the aircraft manufacturer's computers. This is simpler, faster, and more complete. China's economic espionage has moved into cyberspace, is part of normal business practice, reflects deeper problems with the protection of intellectual property, and is so pervasive as to challenge Beijing's ability to control it.

We also need to recognize that many companies have not paid serious attention to securing their networks. There is no obvious incentive for them to do so. This means that it is very easy for Chinese hackers to extract intellectual property from companies in the U.S. and around the world. Once the Chinese discovered this – about a decade ago when global high-speed networks became common, they were quick to exploit the opportunity to move their existing economic espionage programs into cyberspace.

Companies know that their IP is at risk in China but many still estimate that the risk of technology loss is outweighed by economic opportunity. There is an economic rationale for this, in that near term gain for an individual firm outweighs long-term costs, particularly if it takes five years or more for a competing product to appear. But several dubious assumptions underlie this rationale. The illicit acquisition of technology, even if the technology is dated by U.S. standards, helps build Chinese industries and accelerates military modernization. It accelerates improvement in indigenous industrial and technological capabilities, making the recipient better

able to absorb stolen technology and faster at creating competitive products. Companies have underestimated the risk they face, and every Fortune 1000 company in the U.S. has been a target for Chinese hackers who, in many cases, have succeeded in gaining entry and exfiltrating information.

Chinese interlocutors use a variety of reasons to justify these actions. They cite the "Century of Humiliation" when China was carved up by European powers, or the still-overwhelming poverty of many Chinese and the need for growth. Some will say that the U.S. engaged in similar activities in the 19th century when it was a growing economy. None of these excuses makes any sense. The real justification is that China believes it has no choice - politically, economically and militarily - but to take foreign technology.

The Harm to the U.S. and to China

Many discussions of cybersecurity invariably involve exaggeration. The source of this exaggeration is often a lack of specificity in precisely assessing intent, capabilities, and effect. This lack of precision leads to policy recommendations that are either pointless or frivolous. China has the intent to steal intellectual property and its capabilities are more than adequate since American defenses are feeble. China's economic espionage activities against the United States are greater than the economic espionage activities are of all other countries combined. The effect, however, is not one of clear-cut benefit to China. The strategic implications of this theft are difficult to assess. Some call it the greatest transfer of wealth in history; others call it a rounding error for an economy as big as that of the U.S. Neither characterization is correct.

First, it is difficult to estimate the value of intellectual property in the abstract, making it hard to come up with a precise estimate of the dollar value of the loss. Published estimates of the cost to the United States range from a few billion to hundreds of billion of dollars annually. CSIS and McAfee are undertaking a study on how to estimate the cost of all malicious cyber activity, including the theft of IP. Our current estimate is that the cost to the U.S. for all malicious cyber activity, including trade effects, job losses, insurance and recovery costs, fraud, and lost exports is less than 1% of America's GDP.

Second, to utilize stolen technology an opponent must accurately translate complex engineering terms from English to Chinese and then give it to someone with the necessary skills and access to a sufficiently sophisticated industrial base to make use of it. For China, there has been a lag of several years, perhaps as many as ten, between successful acquisition through espionage and the ability to produce competing products (be they military or civil). For simple technologies, it may only take a few months for the Chinese copy to appear; for complex technologies it can take up to a decade. One troubling trend is that this lag time between acquisition and the appearance of a competing product based on stolen technology is decreasing, as China's ability to absorb and utilize technology has increased.

There is no lag between acquisition and use when it comes to confidential business information, which can be used immediately. Theft of oil exploration data, sensitive business negotiation data, or even "insider" stock trading information can be used immediately to make money. The director of an allied intelligence service once described this theft of business confidential

information as a "normal business practice" in China.

China has carefully studied how the U.S. uses technology to increase its military capabilities and has targeted these technologies for acquisition – stealth technology is the best-known example. Chinese espionage has also focused on anti-access capabilities, to deny the U.S. the ability to intervene effectively in Asia. China also takes seriously the discussion in the U.S. of an "Air-Sea Battle" between the U.S. and had undertaken cyber espionage to gain access to relevant technologies, not only to copy them but also to study how they work, in order to be able to neutralize them in combat.

We know that state-sponsored espionage will focus on areas of concern to governments: military and advanced technologies in aerospace, materials, information technology, and sensors, financial data and energy related information. Semiconductors and solar energy have been prime targets. However, government hackers from the PLA and other agencies also engage in cyber espionage as a moneymaking activity and Chinese companies make use of private hackers for purposes of commercial espionage. Private hackers, if they are good, are invited by their local Security Bureau to visit and "drink tea," during which it is suggested that they cooperate in going after certain targets. There is no possible national security benefit to this kind of theft and this is where China's behavior is objectionable.

Most companies prefer to conceal the loss of intellectual property to Chinese hacking, but a few cases have emerged to illustrate its scope. Perhaps the most famous involves Google and several dozen other companies hacked a few years ago – most did not admit publicly to their losses. The Google case illustrates the blend of motives that make Chinese cyber espionage so complex. Chinese hackers looked for information on political dissidents n Gmail. They also examined Gmail to see if the FBI was monitoring the accounts of Chinese agents in the United States. These are legitimate state activities, but the Chinese also took intellectual property related to Google services and products, such as search engine technology, and passed this information to Google's Chinese competitors, an action that violated China's trade commitments to the WTO and to the U.S.

A number of other cases have come to light, including technology taken from Cisco, Nortel, and Motorola – of these only Nortel involved cyber espionage. The current indictment of Chinese competitors for taking technology from Sinovel and American Semiconductor also point to a common pattern. The Chinese government made clean energy technology a priority and clean energy companies in the U.S. became targets. A similar pattern can be detected for the automotive industry and high-speed trains (from Germany and Japan). It is safe to assume that classified information could identify many more cases of U.S. companies that have lost IP to Chinese hackers. China supports its 'strategic industries" identified in China's economic planning and its State-Owned Enterprises through cyber espionage.

The tasking of Chinese espionage and the identification of targets appears to be a diffuse process. There may be general guidelines issued by Beijing, but hackers from the PLA or other Ministries seem to have a great deal of freedom in targeting and in responding to requests for favored companies or research institutions. There are collection targets set by China's military strategy or economic plans, collections to support specific company or military acquisition projects, and

targets of opportunity, where Chinese hackers penetrate a system, come across IP they think is valuable and then transfer or sell it to a favored company.

Chinese claims that the U.S. also engages in economic espionage are ridiculous, if for no other reason that there is little Chinese technology worth stealing. To argue that the U.S. should not object to espionage by China as we did this to Britain is inane – the scale is in no way comparable. The U.S. government did not steal (and does not steal) commercial technology to give to its companies. In addition, the U.S. was a net contributor to the global stock of knowledge in the 19th century, with its citizens creating steamboats, the telegraph, the cotton gin, and countless other inventions that other nations copied freely. The current perpetrators of economic espionage have made no such contribution.

Espionage for national security purposes is a routine aspect of relations among great powers. What is unacceptable is espionage for purely commercial purposes. All great powers engage in espionage against military and political targets. China is no different from any other large nation in doing this, including the United States. Where China's espionage efforts differ significantly from international practice is in the rampant economic espionage carried out by Chinese government entities, including the PLA. Both the U.S. and China would agree that espionage is appropriate to protect national security and advance national interests. Where they would differ is that China sees economic espionage as a legitimate activity to advance its security and interests by securing the technology needed for growth and military power. The broad range of collection targets reflects an official policy to encourage the illicit acquisition of technology as a way to promote economic growth and to modernize China's military forces.

There is also a link between cyber espionage and the development of cyber attack capabilities. Cyber espionage provides, if nothing else, knowledge of potential targets and training for potential attackers. There is also a link between cyber espionage directed at commercial targets and cyber espionage targeted on military technology. It is often the same actors pursuing a collection plan that targets both military and commercial sources – the penetration of RSA was commercial espionage undertaken to enable the penetration of military industrial targets. This report was not tasked with estimating the effect of cyber espionage on U.S. military superiority but a strong case could be made that there has been extensive damage to the U.S. lead in stealth, submarine, missile and nuclear capabilities. We cannot accurately assess the dollar value of the loss in military technology but cyber espionage, including commercial espionage, shifts the terms of engagement in China's favor.

The most troubling aspect of this espionage is that State actors in China, such as the PLA, engage in espionage for reasons of profit. PLA units find commercially valuable information in their quest for military technology and then sell it to Chinese companies. State Owned enterprises can request help from PLA units to hack into a target company's network and then compensate. Many of these activities are outside of Beijing's control, sponsored by politically powerful regional party officials or commanders. This raises the political cost to President Xi of any effort to clamp down. It will also be difficult to change Chinese behavior because if President Xi asks the PLA to stop hacking, he is essentially asking them to stop making money through an activity that many Chinese see as justified. National strategies, politics, and business all combine to make hacking foreign companies to steal technology an attractive proposition.

China is also damaged by the theft of trade secrets and economic espionage. Chinese companies are also victims of hacking by their Chinese competitors. One reason China has no major software company is that no software product can capture market share in a climate of rampant IP theft and piracy. This points to a fundamental tension in Chinese. China is pursuing two contradictory goals. China wants to move up the "value chain of production and, rather than merely assembling other peoples technology, be able to create its own. While much of the technology we use today is assembled in China, it is designed in other nations (principally the U.S., Japan and Germany) and the bulk of the profits go to non-Chinese companies. China is in fact a net importer of technology. It is a long-standing goal of China's leadership to change this, but unchecked cyber espionage undercuts their efforts to create indigenous innovation.

There is an unspoken concern among Chinese policy makers that China does not have the ability to innovate. This is a complex topic best reserved for another discussion but China's "state capitalism" model and its one-party politics likely impedes innovation. Chinese outside of China have no problem innovating, but China's political system and its role in economic decision-making seems to have a chilling effect. China has been willing to invest vast resources to create a national science and technology base capable of supporting innovation far more consistently than the United States, but the political cost of "indigenous innovation" is immense and the pace of change in innovation capabilities may be linked to the pace of political reform.

Discussions with Chinese officials and companies suggest that there is a growing realization in Beijing and elsewhere that weak IP protection is a disincentive to innovation by the Chinese themselves. Some Chinese officials worry that a closed, "techno-nationalist" approach will damage innovation. The emphasis on "indigenous innovation" as it becomes another policy aimed at boosting China's creation of IP that has not delivered adequate results. They realize that they will eventually have to protect intellectual property to help their own companies and their own economy.

Changing China's Behavior

Chinese leaders realize that they face conflicting domestic goals and a serious bilateral problem. Economic espionage provides a technology boost, but puts bilateral relations with the U.S. at risk and hampers China's ability to create indigenous innovation. So far, China has been unwilling to give up its long-running national effort to illicitly acquire technology from Western companies, but action and engagement on this issue by the U.S. and other nations could change calculations of cost and benefit by Chinese leaders.

It is not useful to think of this issue in terms of confrontation, punishment, or conflict. We need a long-term diplomatic strategy linked to our larger goals for Asia and the world. Frustration with the lack of progress in stemming China's activities has led to a variety of bellicose suggestions, few of which make any sense and some of which could actually harm the United States. It is not in our interest to start a military conflict with China, nor is it in our interest to crash the Chinese economy – something that would unleash another global recession. Similarly, a trade war could do more damage to the American economy than cyber-espionage. Hacking back has little real effect, holds real risk of unintended damage, and could start an inadvertent

conflict with China, as the Chinese believe that the U.S. government endorses any private action by Americans. Hacking back runs contrary to U.S. international commitments and to the larger U.S. strategy for making cyberspace more secure.

This is not a new Cold War. We cannot have a Cold War with one of our largest trade partners. The two economies are too intertwined to go back to the rigid, bipolar separation we had with the Soviet Union. There are elements in each country that define the relations in terms of military competition, particularly in the PLA, and Chinese society can be prone to fits of hyper-nationalism, but if China wants to continue to grow and if the U.S. wants to remain a global leader, we have to find ways to cooperate. This will be a difficult process and cyber espionage has become a flashpoint in the relationship.

What the U.S. needs is a broad strategy with four elements. These are a sustained, high level engagement with China on the theft of U.S. intellectual property; the development of measures that will increase U.S. leverage in the engagement process; close coordination with allies, all of whom also suffer from Chinese cyber espionage, to create norms of responsible behavior in cyberspace; and improved domestic cyber defenses to make our companies harder to pillage.

The domestic debate over cybersecurity has not been very useful. There is a tendency to substitute slogans and myths for facts in the discussion of cybersecurity. The result is that after six years of sustained effort by two administrations, we have made insufficient progress in hardening our networks, particularly commercial networks, in the face of Chinese cyber espionage and, of greater concern, Iranian preparations to attack U.S. critical infrastructure. It will be easier for China to give up commercial espionage if the cost of penetrating business networks is increased and the returns from those penetrations are minimized.

Similarly, the U.S. could reduce the risk of Chinese cyber espionage if it had an effective strategy for innovation and productivity growth. It is not that the pace of innovation in China (or any other BRIC nation for that matter) is speeding up. It is that the U.S. is slowing down, largely because of changes in government policy in both Congress and the Executive Branch. In theory, we could change this and reignite productivity growth and innovation. The core of an innovation strategy would be increased federal investment in science and technology and streamlining regulation and tax policy to remove impediments to productivity growth. This is unlikely to happen in the near term, but it remains a possibility. Renewed growth in innovation and productivity in the U.S. would lessen the strategic effect of Chinese cyber espionage.

Since it will be difficult for the U.S. to take the domestic measures needed to manage the risk of Chinese cyber espionage, our efforts now must focus on the diplomatic. In this area, there has been some progress. Last June, the U.S., China and other nations, as part of a UN Group of Government Experts (GGE) on Information Security endorsed the application to cyberspace of the UN Charter, international law, the principle of state responsibility, and national sovereignty. This included agreement that States would not use "proxies" for malicious cyber actions. We know that there are many steps between agreement and implementation when it comes to international practice, but at a recent Track II discussion in Beijing a Chinese official said in a reference to the GGE, that "China's position was evolving in the light of international experience." The U.S. has been working with other nations to build on the success of the GGE

to create norms and agreement on responsible state behavior in cyberspace. As this effort progresses, China's cyber espionage will be difficult to sustain.

Multilateral steps must be reinforced by bilateral work between the U.S. and China. We should expect this process to take years, given the domestic political problems China faces in reining in cyber espionage. In the upcoming Strategic and Economic Dialogue and its subsidiary working groups, we should first expect the Chinese to see if the creation of a working group on cyber issues is enough to placate the Americans – it is a standard ploy on diplomacy and politics to create a Commission to study a problem in order to bury it. They will test how much advantage over the U.S. they can get from the Snowdon revelations - they are unlikely to get much negotiating benefit from his revelation because the U.S. has always told China that military espionage is a two way street and that it is China's commercial espionage that creates problems. What we should expect from this first round is an agreed schedule and an agenda for future talks.

We can find a precedent for how to engage China on cyber espionage in the successful effort to engage China on nonproliferation in the 1990s. The U.S. and it allies created regimes and international norms that established that responsible states did not engage in proliferation. The U.S., supported by its allies, met regularly with Chinese officals to make this point, providing the Chinese with specific examples of objectionable behavior. Every senior US official who went to China made the point that the involvement of Chinese companies in proliferation must stop or it would harm China's relations with the rest of the world. Leaders from European countries, the European Union, and Japan, made the same point – this was particularly important as it demonstrated to the Chinese that this was not solely an American concern. Finally, at appropriate moments in the discussion, the U.S. was able to use or threaten to use a combination of sanctions, including Congressionally-mandated sanctions and other punitive measures to encourage progress.

During the course of discussion with China on economic espionage it may be necessary to consider similar measures, intended to provide leverage and impetus in the discussions, not to punish. The best course would be to use focused measures against individuals or companies identified as being involved in cyber espionage. These could include Treasury sanctions, visa restrictions, and potentially indictments or other trade measures. Any of these measures will face objections from some in the economic and trade communities, but being timid and legalistic will undercut our efforts to get China to change its behavior. At the same time, we need to avoid a rupture in relations or a disruption of trade. We want to encourage China's adherence to international law and agreements. China would benefit as well from better protection of intellectual property and closer adherence to WTO commitments if it wants a larger role in the global economy and its own innovation economy.

The engagement in the 1990s on proliferation is a useful model and evidence that China can be persuaded to change its behavior, but cyber espionage is a more difficult problem than proliferation. Larger economic issues are at stake for both China and the U.S. China is more powerful and more confident that it was two decades ago. Unless the U.S has been careful to build international support for norms of responsible behavior, punitive measures could backfire, and the pace of any discussion will be slower. Our fundamental strategy should be to set global standards for responsible state behavior and then persuade China to change its actions

accordingly. To use a favorite Chinese expression, we must see the talks as pursuing a "win-win" outcome rather than being a "zero sum" game, where for one side to win the other must lose.

The Chinese may be tempted to retaliate – you hear mutterings in China about banning Cisco or other American companies in retaliation for actions against Chinese firms - but it is not in China's interest to start a trade war or further strain bilateral relations. China's economy is weakening. Growth is slowing and China's leaders face a host of problems, including mis-investment, corruption, pollution, and unemployment. Official figures on the Chinese economy are inflated to conceal the extent of the problem. The last thing China need right now is a trade war with the U.S. Nor do the Chinese want to accelerate the trend of foreign investors avoiding the China market. The Chinese hold a significant amount of U.S. debt but it is naive to think this gives them an advantage. For one thing, where else would China put their money – certainly not in Europe or Japan or in their own economy, for that matter? We have to expect the Chinese to test U.S. resolve and must have adequate responses prepared and notified in advance to the Chinese. One element of any U.S. effort would be to warn the Chinese that such retaliation against U.S. firms is unacceptable and risks increased tensions between the two countries.

China's economic growth has been of tremendous benefit to the rest of the world. China has gained, but we have gained as much or more. But what was tolerable when China was an emerging economy is no longer tolerable within it is the world second largest economy. China's economic cyber espionage is a source of instability in the international community and increases the risk of conflict. Cyber espionage lies at the heart of the larger issue of China's integration into the international "system," the norms, practices and obligations that states observe in their dealing with each other and their dealings with the citizens of other states. China can list the justifications as to why it should not be held accountable, but a failure to hold China accountable for cyber espionage undermines efforts to get China to adhere to other international norms and commitments and to find a stable place for it in international relations.

This month's meeting of the Security and Economic Dialogue and its Cyber Working Group are an important first step, but they must be sustained and reinforced with a range of measures, including coordination with allies and improved domestic cyber defenses. Our goal should be sustained engagement to build a cooperative relationship with China that makes cyberspace more secure for all nations.

I thank the Committee for the opportunity to testify and look forward to you questions.