

Cyber Warfare Challenges and the Increasing Use of American and European
Dual-Use Technology for Military Purposes by the People's Republic of China (PRC)

Testimony for the Oversight and Investigations Subcommittee of the Foreign
Affairs Committee of the United States House of Representatives, for its Hearing On:
“Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology”

By Richard D. Fisher, Jr.
Senior Fellow, International Assessment and Strategy Center

April 15, 2011

Mr. Chairman and Distinguished Members of this Committee:

In it appropriate to begin, Mr. Chairman, by noting your consistent leadership in alerting our nation to the multiple challenges to the freedom of all democracies posed by the Chinese Communist Party (CCP). I am also thankful for this Committee for investigating the critical issues of the People's Republic of China's (PRC) ongoing and campaign of cyber warfare against the United States and its use of American technology for military purposes. Both the Internet and dual-use technologies have helped to propel a more globalized world economy, which has produced myriad benefits and thus have many defenders. But I would also submit, Mr. Chairman, that it is time for the United States to devise new defenses against those who are exploiting these benefits to undermine the security of the United States and other democratic nations.

PRC Cyber Challenge

Mr. Chairman, under the leadership of the CCP and as part of its total effort to harness its own cyber realm as a weapon against its citizens, the PRC very likely has built the world's most formidable cyber warfare capability. It is the most formidable in both the breadth of its actors, in its global reach and in the daily threat it poses to America's strategic and economic security. It imposes a heavy financial burden on Americans. A 2009 industry estimate held that annual U.S. cyber security expenditures could reach \$25 billion by 2013. Current open source figures for cybersecurity range from \$10-13 billion per year, slated to rise at 9% a year, or \$1.2 billion -- with cumulative spending under this administration estimated to be \$55 billion for the 2010-2015 period. It is broadly understood that this spending is primarily in reaction to the PRC's cyberespionage efforts. One current estimate asserts that cyber espionage alone costs the United States \$200 billion a year, with, again, the PRC being responsible for most of that burden. According to 11 April 2011 testimony by U.S. Northern Command commander Admiral James Winnefeld, this approaches the national cost of the drug war, estimated at \$181 billion annually. Clearly this challenge is growing.

Earlier this week on 12 April, before the Senate Armed Services Committee, Commander of the U.S. Pacific Command Admiral Robert F. Willard commented on China's cyber challenge saying, “China is pursuing counterspace and cyber capabilities that can be used to not only

disrupt U.S. military operations, but also to threaten the space- and cyber-based information infrastructure that enables international communications and commerce.” In March 2010, Admiral Willard told the same Committee that PRC cyber threats “challenge our ability to operate freely in the cyber commons, which in turn challenges our ability to conduct operations during peacetime and in times of crisis.”

It can be expected that unless the PRC is made to pay a real price for its increasingly aggressive cyber warfare activities, that they will only increase and expand the vulnerabilities of cyber and information-dependent societies like the United States and many other democracies. Measures toward cyber self defense can only go so far barring a change in behavior by the PRC. The CCP’s main motivation for engaging in heightened domestic cyber control and foreign cyber aggression, much as it remains committed to building a level of military power to challenge and exceed that of the United States, dates to the 1989 Tiananmen Massacre. The CCP is pursuing all around global power to deter and defeat all forces that would challenge its dictatorship and regional dominance, to include hostile ideologies like democracy. As the CCP brings to bear all of its cyber, military, economic and political pressures to destroy the nascent democracy on Taiwan, so it will seek to contain, constrain and hold vulnerable democracies in the region and beyond. Cyber warfare will likely remain at the cutting edge of this effort.

PRC Cyber Attack

For well over a decade, computer network attack (CAN), or cyber warfare, has been integrated into the formal order of battle of the conventional military forces of the People’s Liberation Army (PLA). Cyber warfare program also have been pursued by multiple agencies such as the Ministry of State Security (MSS), the Ministry of Public Security (MPS), the Ministry of Information and others. In addition, these “formal” military and intelligence institutions make use of a larger and more amorphous “private” army of cyber warriors in the PRC’s criminal and commercial sector, to include major PRC computer firms like Huawei (the subject of a recent CFIUS case). These capabilities are being developed as weapons which themselves produce strategic effects as well as serving as key force multipliers for conventional “kinetic” warfare operations.

By the early- to mid-1990s one could find a growing vein in PRC military literature on “Information Warfare.” In 1995 then–Major General Wang Pufeng, former Director of the Strategy Department of the Academy of Military Sciences, wrote, “In the near future, information warfare will control the form and the future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China’s military and combat readiness.” Cyber warfare or computer network attack (CAN), is but one aspect of information warfare. In their 1999 book *Unrestricted Warfare*, two PLA Colonels stated, “As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons.”

By early the late 1990s and early 2000s, formal cyber warfare units began appearing in the PLA order of battle. At first a few identified units involved formal trained troops, and also reserve units made up of volunteers from the PRC's corporate computer sector. By 2003 to 2004 there began to appear Special Technical Reconnaissance Units (STRU) in each of the PLA's seven Military Regions, which were believed to be central organizations for the conduct of defensive and offensive cyber operations. More recent orders of battle, however, do not indentify STRU units, which may indicate they have been subsumed within other organizations to better evade attention and detection.

The size of China's potential force of "cyberwarriors" grows even larger when considering the PRC's ongoing cooperation with "cybercriminal" networks and its potential to enlist "allied" support. The Chinese government and its intelligence organs have longstanding relationships with traditional Chinese criminal organizations, or Triads, which cooperate and compete around the world, and are strong in Taiwan, the Asian region and in the United States and Canada. These criminal organizations have been quick to realize profits in cybercrime, and it has been noted that "official" Chinese "cyberwarriors" seek to resemble criminals in their activities. In addition, the PRC's known intelligence cooperation with Cuba, North Korea, Iran, all of which have their own cyber capabilities, presents opportunities for cooperative cyber warfare ventures.

The PRC cyber order of battle also includes government-sponsored "patriotic" hackers and universities. In 2006, one patriotic group, the Red Hacker Alliance, counted 300,000 members. Key PRC centers for Information Warfare and cyber warfare research include the Academy Sciences, the National University of Defense Technology, Tsinghua University and the Harbin Institute of Technology. Foreigners can earn a Bachelors Degree in Information Warfare from the Harbin Institute of Technology and The Guilin University of Electronic Technology. In 2010, Google traced to Chinese universities some of the attacks that drove it from the China market. Cybercrime and cyberespionage clearly are an established line of government investment; criminal and corporate activity; and, academic study and promotion in China.

Cyber Attacks against the United States and Allies

In 2003 the *People's Liberation Army Daily* commented about the need for China to protect its "information territory," which can also be viewed as an indication of what it may target in foreign countries. According to this definition, information territory "not only refers to the Internet in [the] common sense, but also to key information network systems such as finance, electric power, telecommunications, transportation, energy, military and statistics." As the most highly information-intensive society, whose infrastructure is best described as a "system of systems," the United States is particularly vulnerable to information attacks. The Office of Net Assessment estimated that 10% of the US economy is dependent on cyberspace. In the event of a future war with China or involving China's self-declared interests in Asia, the United States should expect that the PLA would use sophisticated computer viruses or "computer bombs" to attack computer systems that control domestic U.S. air traffic, vehicle and rail traffic, emergency control, financial sectors, water, sanitation, and energy. The PLA's goal will be to sow chaos among U.S. civilians while using the same tactics to attack the computer systems necessary for almost every aspect of U.S. military power. It is already the case that U.S. planners and

commanders must consider extant and evolving PRC capabilities to hold the US at risk through aggressive cyber means when contemplating defensive, preemptive or treaty obligations in the Asian region. Already, well short of warfare conditions, the PRC uses the Internet to launch near continuous attacks against the United States and its allies in what might be viewed as a classic asymmetric strategy worthy of Sun Tzu -- turning a US developed asset into a weapon turned against us. Some of these attacks include:

- 2003: China is reported to be the source of most of 294 successful hackings into U.S. Department of Defense computers. China is also accused of entering computers at U.S. Army bases at Aberdeen, where it stole data on the Army's Future Combat System, and intrusions at Fort Bragg and Fort Hood.
- 2003: *National Journal* reports that major portions of the U.S. suffer power outages due to cyber attacks, likely from the PRC.
- August 2005: Reports emerge about "Titan Rain," code name for a group of Chinese Internet spies of uncanny skill who had been tracked by the FBI since 2003, as they broke into multiple U.S. military and defense contractor computers.
- December 2005: Chinese "hackers" reportedly based in Guangdong send personally tailored e-mails to British Parliamentarians intended to launch "spyware" that seeks and sends information back to China.
- January 2006: The first FBI Computer Crime Survey covering 2005 reveals that China is the origin of 25 percent of computer attacks against U.S. businesses.
- June 2006: About 150 Homeland Security Department computers are penetrated and data sent to a Chinese language web site.
- July 2006: China is reported to have broken into the U.S. State Departments computers for the purpose of seizing "information, passwords and other data."
- 2006: China is reported to have attacked and compromised computer systems at the U.S. Naval War College, National Defense University, and the U.S Army's Fort Hood, causing \$20 to \$30 million in damage to each system.
- June 2007: Chinese military hackers are reported to have broken into computer networks serving the U.S. Secretary of Defense, forcing the network to be shut down.
- January 2008: A leaked FBI briefing given in January 2008 reveals their suspicions that uncontrolled or counterfeit CISCO computer routers made in China and widely used by classified U.S. government and military computers may have created large numbers of undetectable "back doors" that could be exploited by PLA hackers.

PRC Cyber Espionage

But short of conditions of kinetic warfare, the PRC uses its cyber capabilities to pursue a relentless global campaign of cyber espionage, in which every country in which the PRC has any kind of interest, is subject to continuous cyber probes seeking all manner of information of military, commercial or political value, while continually seeking new ways to turn a target countries' complex military and civil electronic infrastructure into an Achilles Heel. PRC cyber espionage heavily targets American military and government agencies as well as defense corporations.

The PRC is targeting high value military programs. In April 2009 the *Wall Street Journal* reported that about in 2007, the critical Lockheed-Martin F-35 stealth fighter program had been penetrated by cyber spies, with their suspected origin being the PRC. While other reports sought to downplay the significance of the data theft as not having compromised key combat capabilities of the aircraft, what was unreported is that the PLA may have its own “F-35” like program underway at the Chengdu Aircraft Corporation. So any data about the F-35 would be useful to this program.

Chinese cyber espionage is also suspected to have targeted European military firms. Just this week the French helicopter engine maker Turbomeca was suspected of having been attacked by cyber spies. The PRC was suspected inasmuch as PLA helicopters make extensive use of Turbomeca engines and the PLA would like to copy newer engines more quickly. March 2009: Canada’s Munk Centre reveal “GhostNet,” a PRC-origin cyber spying operation that it tracked infiltrating computers in 103 countries, mainly targeting government computers. 2010: Reportedly because he found insulting data about himself, PRC Politburo Standing Committee Member Li Changchun is reported to have ordered cyber attacks against Google that caused it to leave the PRC market.

PRC Cyber Espionage

As noted, short of conditions of kinetic warfare, in what might be called as stealth war, the PRC uses its cyber capabilities to pursue a relentless global campaign of cyber espionage, in which every country in which the PRC has any kind of interest is subject to continuous cyber probes seeking all manner of information of military, commercial or political value, while continually seeking new ways to turn a target countries’ complex military and civil electronic infrastructure into an Achilles Heel. PRC cyber espionage heavily targets American military and government agencies as well as defense corporations.

The PRC is targeting high value military programs. In April 2009 the *Wall Street Journal* reported that, circa 2007, the critical Lockheed-Martin F-35 stealth fighter program had been penetrated by cyber spies, whose suspected origin was the PRC. While other reports sought to downplay the significance of the data theft as not having compromised key combat capabilities of the aircraft, what was unreported is that the PLA may have its own “F-35” like program underway at the Chengdu Aircraft Corporation. So any data about the F-35 would be useful to this program. Chinese cyber espionage is also suspected to have targeted European military firms. Just this week the French helicopter engine maker Turbomeca cited as having been attacked by cyber spies. The PRC was suspected inasmuch as PLA helicopters make extensive use of Turbomeca engines and the PLA would like to copy newer engines more quickly.

PRC Cyber Control

It is also important to examine how the PRC is exporting its ability to control the internet as a function of preserving its political dictatorship and those of its allies and clients, to include Iran. This, in turn, contributes to the CCP’s ability to manipulate political and economic decisions in those countries and to negatively impact US security In 2000, former President Bill Clinton

stated, "We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China." Well, this change is not altogether positive; the PRC's Internet has been built with the goal of expanding PRC control and censorship of information, its ability to spy on its citizens and prevent disparate pockets of discontented Chinese from unifying toward a decisive challenge to CCP rule.

This is where PRC computer companies like Huawei come to play one active role in expanding the PRC's direct political influence. Huawei began in 1980s as a partnership with the PLA to start building the PRC's national fiber-optic networks, ensuring PRC government control over the growth of the Internet in the PRC. Huawei is now the world's second largest computer hardware maker and has heavily expanded into the cell phone market with its popular "Android" line. Huawei hardware has often been found to carry special software that would allow outsiders to enter into computer networks. Huawei and the PRC's cyber security forces are now exporting their expertise. In Zimbabwe the PRC is reported to be funding the Robert Mugabe School of Intelligence, which will also become a major facility for monitoring domestic computer and phone communication, which is largely carried by networks built by Huawei. By virtue of the presence of PRC technicians and the "backdoors" built into the computer hardware, PRC intelligence services will also maintain a constant intimate understanding of Zimbabwe, helping to ensure that favored political factions will rise to ensure PRC interests in that country, and by extension in any country PRC similarly targets. In this context, PRC's growing presence in the Bolivarian countries of Latin America, including Venezuela, Bolivia and Ecuador bears study.

PRC Use of U.S. Dual-Use Technologies

Mr. Chairman, in addition to cyber espionage, the PRC is also able to gain access or make use of militarily useful U.S. technology for another important reason: we let them obtain it. On June 5, 1989 President George H.W. Bush announced the United States suspension of sales of items on the U.S. munitions list, or an arms embargo, in response to the June 3-4 Tiananmen Massacre in Beijing, China. In 1990 this policy was codified by the U.S. Congress.¹ But almost from its inception successive American presidents have made exceptions to this law, primarily by issuing waivers to allow the purchase of Chinese satellite launch services. In addition, by the mid-1990s the U.S. Commerce Department has allowed a growing trade in so-called "dual-use" items that may have a military use but are not weapons in and of themselves.

For example, in early October 2010 the Obama Administration issued a waiver to allow an unnamed European company to use the U.S. C-130 transport aircraft for anti-pollution work in the PRC. It is suspected that the White House was testing the political waters to see if there was support for further relaxation of technology export restrictions, perhaps to advance its agenda of promoting space cooperation with the PRC.

In 2005 the policy regarding U.S. exports of dual use technologies to the PRC was explained by then Acting Undersecretary for Industry and Security of the Department of Commerce Peter

¹ H.R. 3792, Foreign Relations Authorization Act, Fiscal Years 1990 and 1991, (Considered and Passed by House), <http://thomas.loc.gov/cgi-bin/query/F?c101:1:./temp/~c101LWTHBp:e212825>:

Lickthenbaum, who stated, that “The United States maintains an arms embargo on China. Because dual-use items (such as computers) have important commercial uses, we do not have an embargo on exports of dual-use items to China. However, we have a general policy of denying export license applications for dual-use items to Chinese military end-users.”

But if the goal of this policy is to deny dual-use items to the PRC military, then the policy has not succeeded. Open source information shows that the PLA and China’s People’s Armed Police (PAP) are benefitting from many American made or designed dual-use products. Some, like the AM General Humvee vehicle, were explicitly designed for military use. Others, like jet airliners, utility helicopters, all-terrain vehicles (ATVs) and Segway personal transports may not have been originally designed for military or police use, but are thus used in the West, and now in the PRC. In the case of airliners, it is proving the case that both the United States and Europe have sold the PRC a considerable potential military capability. It seems there is ample cause for some oversight and investigation by the Congress regarding this matter.

One good reason for the Congress to look at how the PLA is using dual use American technologies is that we hope that our allies will follow our example. In the last decade the PRC has exerted great political and economic pressures in European capitals to force an end to the European Union’s 1989 arms embargo against the PRC. At times in the last decade the Bush Administration had to fight hard to keep this embargo in place. This could become more difficult during the current period of financial instability in which some European countries are now dependent on PRC soft loans. For their part, American companies are already upset that Europe’s allowing a greater traffic in dual-use technology to the PRC is creating competitive advantages, pressure the PRC appreciates here in Washington.

This is especially true in the case of helicopter and transport aircraft technologies. Despite the 1989 EU arms embargo Eurocopter has sustained a technology relationship with Chinese helicopter companies, and is now co-developing the EC-175/Z-15 advanced utility helicopter with China. Furthermore, in its rush to secure a greater share of the Chinese airliner market from rival Boeing, Airbus has transferred an airline “kit” assembly line to Tianjin that can only help the PRC advance its own large airliner programs, that will likely be produced in multiple military variants. European marine engines, especially from German market leader MTU, are used in multiple PLA Navy and Coast Guard ships and in PLA Navy submarines. In addition, the European Space Agency is on the record favoring PRC participation in the International Space Station, which would require an extensive review of current U.S. technology export restrictions to the PRC.

What follows is a list of U.S. dual-use technologies that are benefiting PRC military and police forces:

AM General Humvee Light Truck

Though the M998 High Mobility Multipurpose Wheeled Vehicle (HMMWV, or Humvee) is now being supplanted by thousands of more heavily armored Mine Resistant Armor Protected (MRAP) in U.S. service, tens of thousands of this AM General design have entered the U.S.

armed forces and about 45 other countries since the early 1980s. The 1.5 ton Humvee can carry a much greater array of modern weapons and equipment and has been produced in over twenty variants for the U.S. services alone, from utility transport, to ambulance, anti-tank, anti-aircraft, electronic warfare and weather station missions.

The PLA was reportedly very impressed with the Humvee's performance during the first Gulf War and in 1988 AM General was reported to have displayed the Humvee at a military exhibition in Beijing. Other PRC sources have noted that the U.S. Government may have given China a small number in the late 1980s as part of early anti-narcotics cooperation. However, at the 2000 Zhuhai Airshow this analyst noted that a picture of a Humvee-like vehicle appeared in a brochure of the Shenyang Aircraft Corporation. And then at the 2004 Zhuhai show, an actual Shenyang copy was put on display, armed with the TY-90 anti-aircraft missiles. But by this time it was apparent that a second copy was also being produced by the Dong Feng Motors Company, called the EQ2050 "Meng Shi." This version was marketed at the 2005 IDEX show in Abu Dhabi armed with a turret equipped with FN-6 short-range surface-to-air missiles (SAMs) that almost copied the Boeing FIM-92A *Avenger* still in use by the U.S. Army.

Despite repeated inquiries, it was not until early 2008 that an AM General official, on condition of anonymity, explained that the State and Commerce Departments sanctioned the sale and co-production of the civilian H-1 version of the Humvee for the PRC market in the 1997 time frame. This led to a partnership with Dong Feng Motors. It is less clear that there was a formal relationship with the Shenyang Aircraft Corporation. However, the official noted that AM General sells parts to both companies. This official also acknowledged that the PLA and the PRC government are the main customers for these co-produced Humvees and was aware of estimates that Dong Feng may produce up to 1,500 copies. However, neither company has rights to sell versions to the civilian market. According to this same source, in 2007 AM General received a reconfirmation from the Commerce Department of its authorization to sell Humvees to the PRC market.

Currently Dong Feng Motors appears to be the most active producer of Chinese-made Humvee versions. Dong Feng made Humvees apparently use a slightly more powerful diesel engine. One Chinese article suggested that if Dong Feng were to enlist other companies, it could produce up to 100,000 a year for wartime production. So far Chinese-made Humvees have been purchased by Chinese Police departments, the PLA Marines, various PLA Army units to very likely include Airborne and Special Forces units. These would be useful for initial Airborne attacks against Taiwan; the Taiwan military makes extensive use of this vehicle and thus the PLA could cause great tactical confusion. Dong Feng markets a version armed with a roof-mounted 23mm cannon and another Special Forces version armed with a automatic grenade launcher and a squad machine gun. Another version of the Humvee forms the carrier for 81mm automatic mortar and a twin-23mm anti-aircraft gun, and are being used by a novel PLA "Mechanized" Special Forces unit. Dong Feng Humvees were seen participating with PLA Airborne Forces in a mid-June 2008 exercise and also played a prominent role in the October 2010 military parade celebrating the 60th anniversary of the CCP.

Despite the capability that has been transferred to the PLA and the growing threat this presents to U.S. friends like Taiwan, AM General faces tough competition in the China military vehicle market from European automakers. The Italian IVECO designed NJ2046 produced by Chinese partner NAVECO is used by the PLA in several versions, including one for Airborne Forces. The PAP uses one IVECO van version as a mobile lethal-injection prisoner execution platform. Germany's Mercedes Benz has several truck versions in production in China, and the PAP uses an armored Mercedes G-Class vehicle with an anti-sniper detection device.

Helicopters

As it has at various times during the Bush Administration there has been the suggestion that the U.S. relent on Tiananmen related sanctions and permit the sale of spare parts for the 24 Sikorsky S-70 *Blackhawk* helicopters sold to the PLA in the 1980s. Most recently China requested these spare parts for humanitarian concerns related to the S-70's role in relief operations responding to the devastating May 12, 2008 Sichuan earthquake. However, this idea has been repeatedly rejected, in large part due to the S-70s overt military role; this helicopter is regularly seen in PLA exercises carrying artillery and Special Forces vehicles. It will almost certainly be employed in any future operations against Taiwan—which also operates the S-70 and is seeking more.

However, in part due to pressure from the U.S. helicopter industry the Commerce and State Departments have relented in permitting sales of U.S. helicopters to “civilian” Chinese entities. In 2001 United Technologies subsidiary Sikorsky Aircraft Corporation sold S-76 transport helicopters to the Chinese Ministry of Communications, and in 2005 sold S-92 helicopters to China Eastern General Aviation to support offshore oil drilling operations. In 2007 Sikorsky entered into a partnership with Chinese helicopter maker Changhe Aircraft Industries Corporation to co-produce S-76 airframes to support Sikorsky production. In 1998 Sikorsky entered into a partnership with China's AVIC-2 consortium to co-develop the larger S-92 helicopter, and it manufactures the tail of that helicopter. In 2003 Sikorsky established its Chinese partner “Shanghai Sikorsky,” and in 2008 AVIC-2, through its subsidiary Changhe, became a shareholder of Shanghai Sikorsky. Changhe also co-produces the Sikorsky-Schweitzer S-300, a lightweight training helicopter, which also formed the basis for U.S. Navy's Northrop Grumman MQ-8B *Fire Scout* unmanned helicopter.

Another United Technologies subsidiary, the Pratt Whitney Canada aircraft engine maker, sold ten of its PT6C-67C helicopter turboshaft engines in 2000-2001 to assist the Chinese Medium Helicopter program of the Chinese Helicopter Research and Development Institute (CHRDI), the chief designer of China's helicopters. In 2007 Pratt and Whitney Canada claimed they thought they were assisting the “civilian” version of this program, which had been thought to include the 5.5 ton WZ-10 dedicated attack helicopter, and a 6 ton utility helicopter based on the same drive train. The later has yet to materialize, while several prototypes of the Z-10 military attack helicopter are now flying powered by PT6C-67C engines. The Z-10 is about the same size and configuration as the Eurocopter *Tiger*, one of the world's most modern and capable attack helicopters. In late 2010 it was reported that CHRDI may be seeking another engine for the Z-10, but it remains the case that a U.S. engine was used to develop this new weapon for the PLA.

Bell Helicopter Canada, a subsidiary of the American Textron Company, sold its Bell-427 light helicopter in China after 2000, and in 2003 entered into a partnership with Hafei Aviation Industries to manufacture airframes for the Bell-430 helicopter.

However, on a corporate or company level there is a thin-to-no distinction between selling to a “civilian” and a “military” entity in the PRC. All of the PRC’s helicopter companies perform either research and development or manufacturing for the PLA. It is likely that the PRC’s intelligence services have targeted these companies to ensure that PRC companies benefit from data gathered in China, or via cyber espionage operations that could benefit from an understanding of corporate data bases. In addition, all U.S. helicopters sold to “civilian” PRC entities are theoretically subject to emergency military mobilization. This was demonstrated in the response to the May 12 Sichuan earthquake when a S-76 helicopter sold to a “civilian” operator was used along with Russian Mil Mi-17s and European Eurocopter AS-332 helicopters sold to other Chinese “civil” operators. These helicopters are equally likely to be used to support potential Chinese military operations against Taiwan, Japan and India.

PLAAF Boeing B-737-300 Electronic Platform

At the November 2004 Zhuhai Airshow this analyst noticed a peculiar feature in a video presented by the Xian Aircraft Corporation. In a section of the video that showed newly built H-6 bombers outside the Xian factory, there was a Boeing B-737 jet transport with what appeared to be new fairings atop the fuselage. Asian military contacts later disclosed that the PLA had converted two Boeing 737 airliners to serve as electronic control and monitoring platforms to support testing for new long range Land Attack Cruise Missiles. Subsequent Internet-source pictures of the aircraft revealed that new fairings has been placed on top of and on the bottom of the fuselage. Such a configuration could support a command and control or the suggested cruise missile test monitoring mission. A more recent Internet-source photo shows the aircraft to be part of a special PLA Air Force squadron equipped with other electronic and radar test aircraft.

In early 2005 officials in the State and Commerce Departments told Bill Gertz of the *Washington Times* that this PLA use of an American-made aircraft was under investigation. A State Department official reported to Gertz, “...commercial jets are permitted for export to China without a license, but that converting a civilian aircraft into a military jet is not allowed under U.S. export rules.” This official then stated, "It is unquestionably true that these jets could not have been sold to the Chinese military without a presidential waiver, which is very unlikely," Gertz also reported that if China had violated U.S. export rules, “penalties could range from fines to the imposition of economic sanctions on China that would bar purchases of U.S. aircraft worth hundreds of millions of dollars.” However, after nearly six years there has been no action by the State Department or the Commerce Department reacting to this flagrant Chinese military employment of a restricted American technology. Instead, Boeing continues to sell its B-737 airliners to Chinese airlines, which now operate over 200. In 2011 there could be over 500 new Land Attack Cruise Missiles targeting Taiwan. In early 2007 Taiwan’s Ministry of Defense reported that only 100 such PLA cruise missiles were deployed.

PLA Use of American Cargo Airliners for Military Operations

A more ominous use of American made airliners is the PLA's regular incorporation of civilian airliners into military troop and cargo transport missions. The integration of the PRC's civil transport systems into the PLA was made clear by the latest 31 March 2011 PRC Defense White Papers, which stated, "China is working to integrate combat-readiness as an element in the national transportation grid, and improve capabilities in strategic lines of communication support, strategic projection support, and rush transportation and rapid repair."

It has long been known that the PLA uses the PRC's fleet of civilian airliners as a "reserve" air transport resource. These airliners have been used to perform humanitarian and military missions. Following the 12 May 2008 Sichuan earthquake the PLA again used Boeing and Airbus airliners with China Southern and China Eastern airlines to make emergency shipments of personnel and material. These supplemented the use of PLAAF Ilyushin Il-76 and Xian Y-8 transports for the same missions. But then in mid-June 2008, perhaps capitalizing on the need to hone emergency airlift mobilization, the PLA conducted another exercise in which PLAAF Il-76 and both Airbus and Boeing airliners were mobilized to move PLA Airborne troops. The exercise was apparently led by the PLA General Logistics Department, the Beijing Military Region and the China Civil Aviation Authority, which requisitioned civil airliners for the exercise.

However, there was a unique addition to this mid-June exercise: the use of at least one Boeing B-747F and one McDonnell Douglas MD-11F dedicated cargo transports. A cursory count of U.S. made cargo airliners used by PRC airlines—which would now include Hong Kong's airlines-- indicates that they have up to 80 U.S.-made cargoliners. An Il-76 can carry about 48 metric tons while a Boeing B-747F-400 can carry about 55 metric tons. If one accepts current estimates that the PLAAF has about 20 Il-76 cargo transports, then the potential addition of U.S. made cargoliners could potentially quadruple the PLA's air cargo lift capacity. But this is set to increase as Hong Kong's Cathay Airlines has 16 Boeing B-747 cargoliners on order, and China Southern Airlines has six new Boeing B-777 cargoliners on order. The later were quickly put to use in PLA transport exercises help in September 2010.

Enlisting "civilian" cargoliners in potential operations against Taiwan would be very attractive to the PLA. These aircraft could concentrate on moving the wide variety of palletized cargo, from bullets to artillery rockets to beans, that would be needed to sustain light and medium weight tracked and wheeled armored forces that would be best moved by Il-76s. By using civilian cargoliners to build up weapons and supplies, PLA Airborne armored forces sent to capture a Taiwanese airport could quickly move from a defensive to an offensive mission.

Potential Dangers of Space Cooperation with the PRC

Both the European Space Agency and the Russian Space Agency are on the record favoring PRC participation in the International Space Station (ISS). The Administration has been considering this idea but has not yet made a decision as it appears some U.S. officials are fearful that U.S. technology could end up assisting PLA military space ambitions. This fear is well justified. The PLA controls the PRC manned and unmanned space program and ensures that even the manned

space program produces military dual-use benefits for the PLA. All seven of the PRC manned Shenzhou capsule missions have performed some military missions, and both the Tiangong space lab and the larger 60-ton Space Station expected by 2020 likely will perform military missions. Any insights the PLA gathers from its participation in the ISS will likely be applied to its Space Station program, which will better enable its military missions.

The PRC's previous exploitation of the U.S. commercial satellite launch business of the 1990s has already been covered by the 1999 Cox Report and by other analysis. But the PRC's exploitation of the U.S. space program dates even earlier. In 1989, just as the Tiananmen uprising was gathering, a Professor Zhang Litong of the Northwestern Polytechnical University (NPU) was able to secure a Visiting Fellow position at the then NASA Lewis Research Center (now John Glenn Research Center) in Cleveland, Ohio. Two year earlier Zhang had been charged by the PRC government with building its expertise in Ceramic Matrix Composite materials for future spacecraft, especially space planes. The Lewis/Glenn Center is a primary new materials development center for NASA. Zhang took her research back to NPU and has since become famous for circumventing the "embargo" of such technology to the PRC. This past January Zhang was featured on Shaanxi City television explaining her role in helping the PLA build a space plane comparable to the U.S. Air Force's X-37B. It is correct to conclude that the PLA has used Professor Zhang's stint at a NASA laboratory to advance its military space ambitions.

Conclusions

By its aggressive pursuit of cyber warfare and by its aggressive pursuit of European and U.S. dual-use technologies, the PRC is seeking to turn technologies that have aided global economic development, into weapons to advance the power of the PLA. The PRC has turned its ability to control its domestic cyber space into a weapon to prolong its dictatorship and to attack democracies. It is also seeking to acquire U.S. and European aerospace technologies, which already have provided direct contributions to PLA capabilities.

During the Cold War the United States and its allies were able to mount a unified effort that was largely successful in stemming the flow of militarily useful technology to the former Soviet Union, and thus hastened the end of the Cold War. Such a level of protection for U.S. and European technology is opposed by many interests who have benefitted from the PRC's integration into the global economy. But Mr. Chairman, this is where I would suggest that leadership is required. It is imperative that U.S. laws be enforced, or strengthened where they have no effect, to prevent U.S. dual use technologies from creating new military threats. It is also necessary to create a real cost for the PRC's pervasive cyber warfare. Perhaps it is time to consider a formal barring of most Chinese computer products from the American market until such a time that it decides to end this conduct and agree to "rules of the road" with adequate verification.

**United States House of Representatives
Committee on Foreign Affairs**

“TRUTH IN TESTIMONY” DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee require the disclosure of the following information. A copy of this form should be attached to your written testimony and will be made publicly available in electronic format, per House Rules.

1. Name: Richard D. Fisher, Jr.	2. Organization or organizations you are representing: Int'l Assessment and Strategy Center
3. Date of Committee hearing: April 15, 2011	
4. Have <u>you</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	5. Have any of the <u>organizations</u> you are representing received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
6. If you answered yes to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets. 	
7. Signature: 	

Please attach a copy of this form to your written testimony.