COMMUNIST CHINESE CYBER-ATTACKS, CYBER-ESPIONAGE AND THEFT OF AMERICAN TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 15, 2011

Serial No. 112–14

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/

U.S. GOVERNMENT PRINTING OFFICE

65–800PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FOREIGN AFFAIRS

ILEANA ROS-LEHTINEN, Florida, *Chairman*

CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
STEVE CHABOT, Ohio
RON PAUL, Texas
MIKE PENCE, Indiana
JOE WILSON, South Carolina
CONNIE MACK, Florida
JEFF FORTENBERRY, Nebraska
MICHAEL T. MCCAUL, Texas
TED POE, Texas
GUS M. BILIRAKIS, Florida
JEAN SCHMIDT, Ohio
BILL JOHNSON, Ohio
DAVID RIVERA, Florida
MIKE KELLY, Pennsylvania
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
JEFF DUNCAN, South Carolina
ANN MARIE BUERKLE, New York
RENEE ELLMERS, North Carolina
VACANT

HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
BRAD SHERMAN, California
ELIOT L. ENGEL, New York
GREGORY W. MEEKS, New York
RUSS CARNAHAN, Missouri
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
DENNIS CARDOZA, California
BEN CHANDLER, Kentucky
BRIAN HIGGINS, New York
ALLYSON SCHWARTZ, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
FREDERICA WILSON, Florida
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island

YLEEM D.S. POBLETE, *Staff Director*
RICHARD J. KESSLER, *Democratic Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

DANA ROHRABACHER, California, *Chairman*

MIKE KELLY, Pennsylvania
RON PAUL, Texas
TED POE, Texas
DAVID RIVERA, Florida

RUSS CARNAHAN, Missouri
DAVID CICILLINE, Rhode Island
KAREN BASS, California

CONTENTS

Page

WITNESSES

Pat Choate, Ph.D., director, Manufacturing Policy Project 5
Mr. Richard Fisher, senior fellow, Asian Military Affairs, International Assessment and Strategy Center 11
The Honorable Edward Timperlake (former Director, Technology Assessment, International Technology Security, Office of the Secretary of Defense, U.S. Department of Defense) 25
Adam Segal, Ph.D., senior fellow, Council on Foreign Relations 35

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Pat Choate, Ph.D.: Prepared statement 7
Mr. Richard Fisher: Prepared statement 13
The Honorable Edward Timperlake: Prepared statement 27
Adam Segal, Ph.D.: Prepared statement 37

APPENDIX

Hearing notice 50
Hearing minutes 51

COMMUNIST CHINESE CYBER–ATTACKS, CYBER–ESPIONAGE AND THEFT OF AMERICAN TECHNOLOGY

FRIDAY, APRIL 15, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The committee met, pursuant to notice, at 12 o'clock p.m., in room 2172 Rayburn House Office Building, Hon. Dana Rohrabacher (chairman of the subcommittee) presiding.

Mr. ROHRABACHER. I call to order the Subcommittee on Oversight and Investigations of the House Foreign Affairs Committee.

I would like to thank all of you for joining us today. And today we are examining the Communist Chinese cyber-attacks, espionage and theft of American technology.

We will proceed with our opening statements and then introduce the witnesses. And, hopefully, there will be a vote coming up I am afraid, but let us hope we get through the testimony of the witnesses and then we will go and vote and come back and ask the questions.

So, starting off with a Reuters news story this morning reveals that secret U.S. State Department cables trace computer system attacks colorfully code named the Byzantine Hades by U.S. investigators. They have traced these to the Chinese military itself. An April 2009 cable even pinpoints the attacks to a specific unit of the Chinese People's Liberation Army. According to U.S. investigators China has stolen terabytes of sensitive data from password for State Department computers to designs for multi-billion dollar weapon systems.

The United States is under attack.

Cyber-attack and cyber-espionage traced backed to China have been dramatically increasing every year. What kind of damage is being done? How is our national security being compromised? Well shielding our digital infrastructure from attacks, and protecting the intellectual property and classified information is strategically important to our national security. But how do that and what else needs to be done in terms of protecting this?

The Communist Chinese Government has defined us as the enemy. It is buying, building and stealing whatever it takes to contain and destroy us. Again, the Chinese Government has defined us as the enemy.

Chinese cyber-attacks on U.S. assets now number in the thousands every year. The 2009 report on "China's Military Power" published by the Office of the Secretary of Defense notes that, "numerous computer systems around the world, including those owned by the United States Government, continued to be a target of intrusion that appears to have originated within the PRC," end of quote. One of the high value targets that Chinese cyber warriors have repeatedly attacked is the F–35 Joint Strike Fighter program which is the centerpiece of future American air power capabilities.

The heavy use of outsourcing of computer and consumer electronic production to China, not only by American but also by Japanese, Taiwanese, German, and South Korean firms, has helped create a Chinese cyber threat that now compromises the security of the Western world. Beijing has been given technology and a manufacturing base, making Western networks vulnerable to escalating Chinese capabilities.

The Office of the Secretary of Defense in their 2010 annual report to Congress, which was the "Military and Security Developments Involving the People's Republic of China" outlined this challenge. And I quote,

> "The PRC utilizes a large well-organized network of enterprises, defense factories and affiliated research institutes and computer network operations to facilitate the collection of sensitive information and export-controlled technology."

The Chinese often use, and here it is, the term "patriotic hacker" as a cover for their activities, as well as of course corporate spies. But in that dictatorship the line between state and private efforts is blurred intentionally to give Beijing plausible deniability.

Chinese thinking is based on slogans such as "Give Priority to Military Products," and "Combine the Military with the Civil." Thus, economic and commercial spying and theft are most frequently connected with tech-heavy industries deemed to be strategic to the regime. This includes computer software and hardware, biotechnology, aerospace, telecommunications, transportation, engine technology, automobiles, machine tools, energy, materials and coating.

A new study by the RAND Corporation, which it was "Ready for Takeoff: China's Advancing Aerospace Industry," that report found, and I quote,

> "China's aerospace industry has advanced at an impressive rate over the past decade, partly due to the increasing participation of its aerospace industry in the global commercial aerospace market and the supply chains of the world's leading aerospace firms . . . China's growing civilian aerospace capabilities are unquestionably contributing to the development of its military aerospace capabilities."

Combine these commercial transfers with the espionage committed against American military programs like the F–35, and no one should be surprised by the roll out of the new J–20 "stealth" Chinese airplane last January. It was years ahead of what all the experts predicted that China was able to do on its own.

It is what happens during "peace time" that determines the balance of power and governs the outcome when that peace breaks down. National security must be a constant concern.

Battleships and mass armies were left behind by aircraft carriers and rockets. Now we must understand that today's threat emanating from cyberspace and technology transfers as well as from traditional practices of espionage.

Today we have before us four experts on the connection of technology transfers and national power in a competitive world.

Mr. Pat Choate is currently the director of the Manufacturing Policy Project, a private, nonprofit institution. Mr. Choate has written widely and several books, including "Agents of Influence" and the "The High Flex Society," which document the decline in America's competitiveness and the influence of foreign powers right here in Washington, DC.

Mr. Richard Fisher is a senior fellow with the International Assessment and Strategy Center. He is an active writer and a scholar on China having worked for the Jamestown Foundation, the Center for Security Policy, and The Heritage Foundation. He is the author of "China's Military Modernization, Building for Regional and Global Reach," and has been published in numerous newspapers and professional journals.

Mr. Edward Timperlake served as Director of Technology Assessment, International Technology Security for the Department of Defense from 2003 to 2009. He identified and protected the Defense Department from espionage, that was his job and we're anxious to hear more about that. He also served as the Department of Defense's representative to the National Counterintelligence Executive Committee. Before that he graduated from the Naval Academy and served as a Marine fighter pilot, as my dad did for 23 years. And co-authored the book, "Showdown: Why China Wants War with the United States."

And finally, we have Mr. Adam Segal, a senior fellow with the Council on Foreign Relations and an expert on security issues and China policy. He has recently written a book entitled, "Advantage: How American Innovation Can Overcome he Asian Challenge." He has taught Vassar College and Columbia University. He holds a Ph.D. from Cornell.

I want to thank all my witnesses, or our witnesses for being here today.

And now we'll have opening remarks from our members, and then we will proceed with your testimony.

Mr. Carnahan.

Mr. CARNAHAN. Thank you, Mr. Chairman for holding this hearing. And I want to compliment on the interesting and timely subjects that you have brought to this subcommittee. And we look forward to continuing this work together.

As the U.S. economy continues to recover, we must do everything we can to create jobs here at home and support domestic manufacturing.

As of 2010, China was the world's third largest buyer of products from my home state of Missouri ranging from machinery, pharmacueticals, agriculture products. We experienced a 43-percent growth in exports from Missouri to China. Nearly $1 billion

sales last year alone. Missouri made products exported to China that are creating jobs here at home in the midwest and beyond.

With nearly 20 percent of the world's population, the Chinese market represents an opportunity for American business to create job here at home by making American products at home and exporting them to China, but here's the "but." This growth, while it is an opportunity, it cannot and will not reach its full potential so long as American companies remain at risk. Given the long running efforts to illicitly acquire technology from Western companies, and a lack of protection of intellectual property rights there is a significant limitation to the export growth potential of U.S. corporations.

While it is in our economic and security interest clearly to counter any and all of these issues, it is also in China's best interest to come to the table and address them in a serious way. China itself is increasingly susceptible to hacking and cyber crime and theft of intellectual property by others around the world, especially given that its technology is not as superior as ours. It is in the best interest of both countries to diplomatically address these issues and encourage Chinese officials to come to the table to do just that: Address these issues in a serious way.

I look forward to hearing from our witnesses today. And I yield back, Mr. Chairman.

Mr. ROHRABACHER. Thank you very much.

And we have with us, I am going to see if I am pronouncing right, David Cicilline?

Mr. CICILLINE. Yes.

Mr. ROHRABACHER. And you're from Rhode Island. And we would recognize you for an opening statement.

Mr. CICILLINE. Just thank you, Mr. Chairman. I just would like to welcome the witnesses and thank the chairman for scheduling this hearing.

This issue of how do we support American manufacturers and deal with the very real issue of the theft in intellectual property is of great interest to me and to my constituents, and to our country. And I am particularly also interested in hearing the witnesses' testimony on what we might do to further enhance cyber security.

So, I welcome you and thank you for being here today.

Mr. ROHRABACHER. Thank you very much. Welcome to the subcommittee.

Mr. Choate?

Mr. CHOATE. Mr. Chairman, members——

Mr. ROHRABACHER. I am sorry. I was trying to figure out how to pronounce his name so much that I did not even see him there.

And another one of our new members, Ms. Bass. No, if you have an opening statement, please feel free.

Ms. BASS. Thank you for holding this hearing. And I am also very interested in the testimony that you have to say, and a particular interest, I mean in addition to the cyber-attacks, is the whole idea of the problem in China with piracy. I know that is not the topic today, but hopefully in a future hearing we will be addressing that.

Mr. ROHRABACHER. Thank you very much.

You have a very easy name to pronounce. All my life with a name Rohrabacher I have got to pay attention to pronunciations.

Mr. Choate, go right ahead.

STATEMENT OF PAT CHOATE, PH.D., DIRECTOR, MANUFACTURING POLICY PROJECT

Mr. CHOATE. Thank you, Mr. Chairman, members of the committee.

Let me focus my comments on how the United States actually facilitates such cyber-espionage and talk about things that we can do here at home in dealing with it.

Chinese cyber-attacks, of course, are massive, there have been numerous studies that have identified these attacks. We know that all of our major agencies, corporations, banks, research and other entities are subject to these attacks.

The greatest concentration of technology, of new technologies, advanced technologies in the world is at the U.S. Patent Office. What we have each year is 500,000-plus applications from around the world, about half of those applications are foreign-based but half are from the United States, seeking a patent. And at the Patent Office what we have is a situation in which we have probably the oldest computers in the Federal Government are found at the Patent Office. There have been a number of comments on that by Mr. David Kappos, who is the Director of the US PTO.

Another basic principle that we can assume: Anything that is on the internet can be hacked into, whether it is our IPhone or whether it is our personal computer, or our IPod that is connected.

So, we have to assume that the Patent Office is regularly hacked into and the best information is taken from the Patent Office. I do not think that has received the attention that it merits.

The second thing that happens in talking to computer security experts, and I have done this for a couple of books, is the first thing that a foreign intruder seeks is to identify the sources of this technology.

If you go into the Patent Office, or if you just simply take the published Patent applications, you can narrow down the fields to those companies that are doing the most advanced research, large and small. Then once those companies are identified, the Chinese are particularly effective at doing a barrage of attacks upon the computer systems of those companies in an attempt to put in Trojan spyware that will enable them at the schedule of the intruder to produce the information of the company itself and literally on an hourly or daily basis, they know exactly what is going on with the technology or research there. The issue is one of how do we improve the security of information in that process.

A second issue that I mention in my testimony relates to the entire question of the security of economic technology. We have both national and economic security needs in this country. We have laws on the books that deal with the national security, the military technology. We have laws that require the imposition of secrecy orders. We have no such laws on economic technology. And increasingly what has happened over the years is we have dual technologies that are used for both purposes.

In the back of my testimony I have a table that I would direct your attention to on the number of secrecy orders that have been given. It's the fifth column over.

And what we see in during the Cold War era we would have hundreds of items each year that would be put under a secrecy order. A patent would be given, but the secrecy would not be allowed. That rate has declined by about 90 percent in recent years.

Last year there were 86 secrecy orders issued at the Patent Office. Of those, about 60 were from the National Labs and dealt with atomic issues. There were about 26 John Doe secrecy orders imposed.

Now here's the problem. We have the Department of Commerce, the Department of Defense, Department of State, Homeland Security imposing export controls on certain technologies because we do not want people who might be hostile to us to have that technology. At the same time, we are putting up through the Patent Office on the internet the patent applications and the full patent itself which includes the best mode for the best way to make it. So simultaneously we are losing billions of dollars of sales and we have absolutely no security benefit from that.

So, I think this is a very rich area of study of how do we take our national security and recognize the dual use technologies? How do we make sure that we have an improved security inside the Patent Office on this publication of materials?

Thank you, and I look forward to your questions later.

[The prepared statement of Mr. Choate follows:]

Testimony
of
Pat Choate
Director, The Manufacturing Policy Project

"Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology"

Before

The Oversight & Investigations Subcommittee
The House Committee on Foreign Affairs
United States Congress
Washington, D.C.
April 15, 2011

Mr. Chairman and Members of the Committee:

My name is Pat Choate. I direct The Manufacturing Policy Project, a non-profit public policy research institute that studies the U.S. and global economy. I am pleased to share some thoughts with you on "Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology."

I will limit my comments to Cyber-Espionage and the effects of existing patent publication policies on U.S. economic and national security.

The Internet and Espionage

The Internet is now the principal tool of modern espionage. Cyber-spying allows intruders to place Trojan horse software inside target computers. This spy ware is most often undetectable to operators, the system and any cyber guards. The mission of this software is to send proprietary information back to the cyber spy on whatever schedules the intruder desires.

While China's companies and governments are major sources of cyber-spying, they are hardly alone. Interviews with cyber security experts, both in and out of the federal government, reveal that many other nations do the same, though not on the same scale as China.

The economics of cyber-theft is simple: Stealing technology is far easier and cheaper than doing original research and development. It is also far less risky to the spy than historic cloak and dagger economic espionage.

A major problem for cyber-spies working in the U.S. with its rich technology base is the identification of the most promising targets. The U.S. government assists in that selection process by requiring the Patent Office to post on the Internet patent applications 18 months after the filing date. Thus, in one place, -- the open computers of the U.S. Patent Office -- a cyber spy can find virtually all the newest, cutting-edge U.S. technologies in virtually any field.

Once the cyber-spy has identified an inventor or company with worthy technology, the spy can then concentrate on stealing all of their technology secrets. Computer security experts report that these targeted inventors can expect a continuing barrage of cyber-spy attempts, sometimes 50 per day, until their cyber security is penetrated.

Cyber-spying can be a lucrative business. Many private firms now exist that will cyber-spy for a contracted fee, no questions asked.

The only sure defense against such intrusions, many security experts say, is to unhook a secure computer from the Internet and transfer data in ways that will not be vulnerable to any Internet connection.

Mandated Revelations of Technology Secrets

The idea of a patent is simple. Someone has an idea for a new creation. If they will share fully their knowledge of it, society will grant them exclusive use for a limited time.

Until the fall of 2001, the Patent Office was required to keep secret all the details in a patent application. If it granted a patent, the information was made public. If the Patent Office rejected the request for a patent grant, it destroyed the application and the inventor could try again or use the creation as a trade secret.

The Patent Act of 1999 altered this 210-year relationship between inventors and society. It required the Patent Office to publish patent application 18 months after the earliest filing. The only exception was for those inventors who agreed not to seek a foreign patent.

Suddenly, the Patent Office was required to reveal to the world the inventor's secrets, including the best mode of creating it. In addition, if the patent was rejected, which now happens with about half of all applications, the inventor's

information became prior art available to anyone, anywhere in the world at no cost.

Since 2001, the Patent Office has made public massive amounts of information about applications that have are not yet been processed. In the period FY 2001 through FY 2010, the U.S. Patent Office published more than 2.3 million patent applications. Of these about half came from U.S. inventors and companies and about half came from other nations that also require publication at 18-months after filing.

These mandated publication requirements make cyber-spying ridiculously easy. All another nation or foreign corporation need do is place engineers at a high-speed Internet terminal and have them harvest the technology disclosed as part of the patent process. In conducting this information gathering, the intruder can locate cutting-edge work by inventors, large and small, and then target them with cyber attacks designed to penetrate their computers.

While it is tempting to blame foreign corporations and governments for such technology theft, ultimately they are not responsible for our stupidity in making it so easy.

Secrecy and Export Controls

The Patent Office and numerous other Departments have a long experience that goes back to World War I in restricting the proliferation of technologies that might affect our national security and the issuance of secrecy orders that prevent vital technologies from slipping into the hands of those hostile to the United States.

Today, however, the USPTO lacks the ability to protect the economic security interests of the nation because it lacks the authority to refuse the grant of the license to file for a foreign patent on economically sensitive technologies. In a world in which the distinctions between military and civilian uses of technology are quickly disappearing, national and economic security is complexly entwined, often indistinguishable.

While agencies, such as the Commerce Department's Bureau of Industry and Security, the State Department, Homeland Security and the Defense Department, can impose export controls on economically sensitive technologies, the USPTO in effect undermines those controls by publishing the patent application, and later the patent itself, on the Internet. Many foreign producers can take this information and duplicate the technology. Thus, the United States loses export sales, even as it makes available to anyone in the world all the secrets of vital

technologies.

While the requirement that no patent or application subject to a secrecy order is to be published protects national security, economic security cannot be similarly defended because of the existing publication rules. It is a major gap in our economic and national security since so many technologies are dual use in nature. Any remedy is likely to require legislation. Certainly, it will require changes in present administrative procedures.

The issue is not one of agency or administrative failure at the Patent Office or any other federal department, but one of a structural gap created by the 1999 Patent Act. This gap merits immediate examination and would ideally focus upon creating:

1. The legal authority, rules and procedures for the USPTO and other agencies to screen applications for foreign filing licenses that implicate economic security concerns.

2. A unified package of criteria to be used by the USPTO and those screening export of economic security technologies, including a declassified version of the criteria that would be made publicly available.

3. More transparency in the process of screening patent applications for both national security and economic security concerns, including the publication of annual statistics on the number of secrecy orders and foreign export control filing licenses.

4. Arrangements with other nations that impose an 18-month publication requirement to permit some summary, such as the 150-word abstract that is part of each patent application, but reveal no details of the creation.

As events have repeatedly illustrated, America has enemies. In this hostile world, our economic security is as important as our national security, and increasingly the two are the same. The existing, unfocused publication policies are a fundamental threat to our security, national and economic, and this requires repair as quickly as possible.

Thank you, Mr. Chairman.

Mr. ROHRABACHER. Thank you very much, Mr. Choate. And appreciate you keeping it within 5 minutes, and we will have a longer session to ask questions and answers after that.

Mr. Fisher?

STATEMENT OF MR. RICHARD FISHER, SENIOR FELLOW, ASIAN MILITARY AFFAIRS, INTERNATIONAL ASSESSMENT AND STRATEGY CENTER

Mr. FISHER. Chairman Rohrabacher, I would like to begin by thanking you for your consistent leadership in helping to alert this nation to the threat from China's Communist Party. And Chairman Carnahan and other members, I would like to extend my thanks to you for holding this hearing today.

Both the internet and the dual use technologies that I will cover in my remarks have helped to propel a far more globalized world economy which has produced myriad benefits, has 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 and harming of the security of the United States.

In my testimony one of the major points that I make is to highlight the cost of China's cyber warfare against this country. I have provided some figures in a PowerPoint slide and that looks at, at least, open source estimates of annual expenditures. And last year I found an estimate that describes the cost of just cyber-espionage alone as mounting to almost $200 billion a year. This is comparable to what the United States is spending to defend ourselves or what is the cost of the impact of the war against in this hemisphere.

Admiral Winnefeld just 3 days ago provided the figure of $181 billion as he impact on this country of the war on drugs.

So with that level of importance, that level of comparison, I think a far greater degree of public focus needs to be placed on this challenge of Chinese cyber warfare.

In my testimony I describe some points about the order of battle that PLA has put together, how cyber warriors or drawn from the criminal sector, from the computer industry. You mentioned the Reuters story today that described a U.S. Embassy cable that has traced attacks back to a specific unit in Chengdu. The Chinese have a cyber army that is fully integrated into their order of battle. What we need to do to defend ourselves is another long and complex subject, but at minimum we need to consider how we can raise this issue in importance in terms of the information that we share with American citizens.

Every year at the Pentagon, because of the Congress, has to print a report about PLA modernization, Chinese military modernization. I believe that we need a similar report that highlights China's cyber war against the United States and all other democracies.

Now I'd like to move on to looking at how American dual use technologies are being used by China increasingly for military purposes. I have written on this at some length in the past, and I put together just a few PowerPoint slides that provide some examples.

Early in the last decade two Chinese companies basically stole the AM General Humvee and put it into production. One company, the Dong Feng Motor Company is now producing this vehicle for

the People's Liberation Army and the People's Armed Police. It's not something that AM General would talk to me about until just a few years ago. And it apparently is something that happens with the approval of the Commerce Department. And it does not appear that there is anyone who is aware or taking any action to address an American-designed vehicle being used by the Chinese military.

Another example that I discovered at a Chinese air show in 2004 was that two Boeing 737s have essentially been dragooned into the People's Liberation Army Air Force. My sources in another country explained to me soon after that these airplanes were being used in China's Cruise missile development program. There are now 400, 500, 600 Cruise missiles appointed at Taiwan, and this aircraft helped to develop them.

Here we see at the far left the 737s and Chinese electronic warfare and electronic technology development unit.

Here we have another problem, and that is how China has integrated the airliners and the cargo liners that we have sold them into a civilian reserve force that is now helping to transport PLA troops and forces, and equipment. This is an exercise that took place in 2008, a U.S. built Boeing 747, a McDonnell Douglas DC–10 and we see Humvees being arrayed as part of the forces being transported.

This is an exercise that took place last year. China Southern Airlines just acquired this Boeing 777F and promptly went into a mobility exercise.

Finally, there is the problem of how to control academic research, especially when it has a military use. I included in my testimony an explanation of the case of a certain professor who was allowed or invited to be a visiting fellow with a NASA Laboratory in the late 1980s. She then returned to China with her information and became a leading expert for China in the development of composite ceramic matrix materials which are used to shield spacecraft. And she is now involved in China's effort to build military spacecraft and military hypersonic products.

I do not think that there is enough of an awareness or a willingness on the part of those who should be defending our technology, and that would be my final point, sir.

Thank you very much.

[The prepared statement of Mr. Fisher follows:]

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 is 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, it 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 wavers 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 relation 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 in 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 Easter General Aviation to support offshore oil drilling operations. In 2007 Sikorsky entered into a partnership with Chinese helicopter maker Change 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, though its subsidiary Change, became a shareholder of Shanghai Sikorsky. Change 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 quaduple 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.

Mr. ROHRABACHER. Thank you very much, Mr. Fisher. We will get back to you during the questions and answer. But it appears that we are spending a lot of money on research and development here and maybe the benefit is going overseas. But we will let our next witnesses comment on that as well.

Mr. Timperlake?

STATEMENT OF THE HONORABLE EDWARD TIMPERLAKE (FORMER DIRECTOR, TECHNOLOGY ASSESSMENT, INTERNATIONAL TECHNOLOGY SECURITY, OFFICE OF THE SECRETARY OF DEFENSE, U.S. DEPARTMENT OF DEFENSE)

Mr. TIMPERLAKE. Thank you very much, Mr. Chairman, distinguished members.

I would like to submit my testimony for the record and summarize briefly.

The 106th Congress of the First Session reported out a bipartisan document that is a tribute to the fact that the U.S. Congress in national security concerns come together as one, it was called the Cox Report. It was a report on the activities of the People's Republic of China. I linked it in my testimony. Anybody that reads that can go to the Congressional Web site or buy a copy on Amazon. Read it, look at today's headlines to check and see the lineage of what they went after and where it is today. I picked three quick examples.

In the '90s, the People's Republic of China targeted ballistic missiles. Sure enough, they also proliferate, by the way. Boom goes the dynamite on January 11, 2007 they successfully kinetically killed one of their satellites. Some day that may be seen as the precursor to the opening round of a quasi-war in space.

They went after high performance computers. I looked that up, and in 1999/2000 I think Saudi Arabia and Portugal were ahead of China, we had the top nine out of the ten, Japan was closing. And again on 20 October the BBC announced that China now has the top super computer in the world. So, they got that one.

Stealth and composite technology, they went after that. Sure enough, as you mentioned, they rolled out the J–20 Annihilator and embarrassed everybody. Previous to that the Russians flew their F–22ski, the TF–50. Both of them were a test flight that caught several by surprise. Three Air Force officers did not see it that way, General Corely U.S. Air Force, Lieutenant General Deptula of the Air Force Head of Intelligence, and General Thomas McInerney. Unfortunately, the F–22 was stopped at 187 Raptors, and I think that was a strategic blunder which tell us we have to protect the F–35 at all cost because that is our ace in the hole coming in combat maneuvering in the future.

Concurrently while the Chinese were spying, they did the "Revolution in Military Affairs," they saw Andrew Marshall publish this great document in which Mr. Marshall, director of Net Assessment, said here was two evolutionary technologies: Precision-guided munitions and remote sensors, and information war.

The Chinese military literature tells us in the late '90s they were giving doctorates in information war. The term "cyber" had not been in vogue at that time, so they really got off the dime very quickly on that.

I would argue though, and we will discuss this, that the PRC actually has two cyber enemies. They have the free world for whatever they can get, and the other one is their own people. And they are very concerned about that, so that compounds their problem and is an area that we can exploit.

There are two case studies I presented. The first one was the Varyag, the aircraft carrier, that's denial and deception. They sent a team over to buy it, it was a cold war relic. And they claimed that they were purchasing an aircraft carrier to be a casino Macau. They got though the Turkish Straits of the Bosphorus by that cover story. Sure enough, very recently Xinhua is on saying "The huge warship on the verge of fitting out, is fulfilling 70 years of China's dreams for an aircraft carrier." I would say that basically they named it the Shi Lang after the Ming Dynasty admiral. I'd rather call it the Casino, because that's how they said hey were going to use it.

The other case is they send bad things to bad people. Whenever the Chinese Government gets something, they have a 16 character policy which says: We get it, we filter it through the use and the need for the state. And in doing so it's a brilliant strategy. They then perfect it and balance it by proliferation. I went to Iraq, I looked at all the Chinese weaponry that were oil for food violations, and sure enough I listed them in my report. In addition, Huawei a Chinese firm was in pre-war Iraq, post-war Iraq. And I was looking at the CPA, I was engaged with that. I noticed on the Web site they were bragging that they had gotten into Iraq and basically that was prohibited. In my personal opinion Huawei is an ongoing criminal operation as much as anything.

How are we doing and what are we doing about it? The Justice Department formed up a task force in 2007 to focus on this. They have done a magnificent job. I give a link to that. I even gave some of their press releases on spy cases they have busted, and they really are making these cases.

Finally, the issue of cyber security; it's a black swan event, which is a great book. Basically, expect the unexpected, the highly improbable. And we formed up the U.S. Cyber Command. I want to give Mike Wynne a credit to his vision, the Billy Mitchell of our generation. He saw the need early with the U.S. Air Force Cyber Command that melded into the bigger cyber command picture.

I really do believe that we as Americans have a challenge but we will, because of hearings like this, address that challenge.

Thank you, sir.

[The prepared statement of Mr. Timperlake follows:]

Edward Timperlake
Managing Editor SldForum.com
Friday April 15, 2011

House Committee on Foreign Affairs
Oversight and Investigations Subcommittee

"Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology"

Testimony on cyber-attacks, espionage, and technology transfers to the People's Republic of China, before the Foreign Affairs Committee, United States House of Representatives.

Mr. Chairman and distinguished members of the Committee, it is an honor to be asked to testify on such an important subject. I have prepared this written documentation of past and current activities of agents of the Peoples Republic of China (PRC) who conduct espionage operations against the United States of America. Tragically, agents of the PRC have had some notable success.

Mr. Chairman I will summarize my prepared statement.

The history of Peoples Liberation Army (PLA) espionage attempts against US military and dual-use technology in the nineties were identified and reported on by a Select Committee of the House of Representatives. The Congressional report is a tribute to the tremendous bipartisan effort of those Members who served because the final report was voted out unanimously:

- **"U.S. National Security and Military/Commercial Concerns with the People's Republic of China," Declassified Report issued, May 25,1999 106th Congress, 1st Session.**

The late Chairman Solomon of the House Committee on Rules established this select Committee under the direction of the Speaker because of the clear and present danger of illegal foreign money entering the American Political process. It can be seen in its entirety at www.house.gov/coxreport/ or at Amizon.com "The Cox Report."

All types of individuals were giving money to the American political process, from drug dealers, Russian Mafia to PLA espionage agents. It was a dangerous and nasty time and America is still living with the consequences of those days.

The PRC had an agenda to not only curry favor with agents of influence but also collect information and conduct espionage operations, a select Congressional committee was created. The extensive report issued by that committee covered significant aspects of US military and commercial dual-use technology that was targeted by PRC collectors. The PRC agents success in the 90s and continuing to this day is being seen in the continued rapid modernization of all military forces of the Peoples Liberation Army.

For brevity I have pulled out a few representative samples in this overview of the PLA's current clear and present threat to America's National Security. I am using "PLA" as a catch all for PRC Army, Navy, Air Force, 2nd Artillery, Cyber and Space forces.

A significant number of technologies which are now in the current PLA inventory were identified as potential problem areas by Congress over a decade ago. We are living today with the rapid modernization of all PLA forces originating from mistakes made in the 90s.

The representative technology I picked is associated with Ballistic Missiles, Super-Computers and Stealth. *(Report language I chose is in italics)*

First, the key point to understanding espionage by the PRC is to recognize their National Security "16 Character Policy."

The PRC 16-Character Policy is to "Give Priority to Military Products"
• *Jun-min jiehe (Combine the military and civil)*
• *Ping-zhan jiehe (Combine peace and war)*
• *Jun-pin youxian (Give priority to military products)*
• *Yi min yan jun (Let the civil support the military)*

Ballistic missile technology:

- *The PRC has stolen U.S. missile technology and exploited it for the PRC's own ballistic missile applications.*
- *In the late 1990s, the PRC stole or illegally obtained U.S. developmental and research technology that, if taken to successful conclusion, could be used to attack U.S. satellites and submarines.*
- *The PRC has proliferated such military technology to a number of other countries, including regimes hostile to the United States.*

Iran --The PRC has provided Iran with ballistic missile technology, including guidance components and the recent transfer of telemetry equipment. The PRC reportedly is providing Iran with solid-propellant missile technology. Additionally, the PRC provided Iran with the 95-mile range CSS-8 ballistic missile. The PRC has also provided assistance to Iran's nuclear programs

North Korea-- The Select Committee judges that the PRC has assisted weapons and military-related programs in North Korea.

- My Comment---On January 11 2007 the PLA successfully attacked and kinetically killed one of their satellites in orbit.

High Performance (HPCs) or "Super Computers"

HPCs from the United States have been obtained by PRC organizations involved in the research and development of:

• *Missiles*
• *Satellites*
• *Spacecraft*
• *Submarines*
• *Aircraft*
• *Military systems components*
• *Command and control Communications*
• *Microwave and laser sensors*

- My Comment--On 28 October 2010 the BBC announced that China has claimed top spot on world's Super Computer List—Their Tianhe-1A (Milky Way) can carry out more then 2.5 thousand trillion calculations a second.

Stealth and Composite Technologies

What is stealth? Simply put, stealth is the ability to conceal an attacker from a defender's detection and defensive systems, and successfully accomplish the mission. To avoid detection, it is necessary to reduce or eliminate the attacker's "signature." The "signature" is composed of five primary elements:

• *Visual signature*
• *Infrared (heat) signature*
• *Acoustic (noise) signature*
• *Radio transmission signature*
• *Radar signature*

In my research I have found often that PLA weapon development efforts can go "dark" for five to seven years. PLA forces, after perfecting their purloined technology and adding homegrown technology can then surprise the world on their technological advancements. The recent rollout and test flight of the J-20 follows this pattern.

- My Comments---Recently the Peoples Liberation Air Force surprised our Secretary of Defense and the American Intelligence Community when their PLAAF Fighter the J-20 "Annihilator," had its initial test flight.
- Congress anticipated this emerging capability over a decade ago and yet in 2011 the PLAAF still surprised the world.
- To be fair, General Corley, USAF, LtGen. Dave Deptula USAF, and LtGen. Thomas McInerney, USAF anticipated this event.
- Unfortunately, this rapidly emerging J-20 threat, along with the slightly earlier 5th Gen Russian Sukhoi T-50's test flight, were not seen early enough by the US Intelligence Community. Consequently, in October 2009, funding for the continuing F-22 production line was stopped at 187 Raptors because at that moment the F-22 was declared both "outdated" and no threat was seen on the horizon.

The Revolution in Military Affairs and Cyber War

While Congress was researching the issues mentioned above in the late 90s, Mr. Andrew Marshall Director of Net Assessment, Office of the Secretary of Defense, published his

short and very direct paper heralding the advent of a "Revolution in Military Affairs." The PLA and especially their spymasters were paying close attention.

Mr. Marshall's vision was profoundly simple. He postulated that technology and war fighting would evolve toward two constantly improving military capabilities.

- Precision-guided munitions with remote sensors
- Information war (the word "cyber" had not yet come into vogue)

In developing their "Information War" military doctrine, the PLA was awarding Doctorates in Information War to military officers as early as 1998. Since that time PRC cyber espionage attempts have been growing and are unrelenting.

Traditionally the commonly accepted thoughts about PRC espionage is that they have different "spy craft" then the "cold war Russian" model of linear cells and cut outs. The evidence in the 90s is that the PLA approached collecting information and technology much differentially than the Russian "cold war" model.

It has been my experience in investigating illegal money contributions that the PLA as needed will use their military along with their Intel community professionals, criminal elements (Triads), businessmen "hustlers," academics both professors and students and even relatives of all those groups—what ever works.

So when the world become more digitized through the computer revolution, the PLA adapted, and became world class offensive cyber war fighters. However, this time there was a role reversal from Russian cyber activity. Russian cyber activity has been reported to be very wide open ranging from military and state sponsored activity, to numerous criminal enterprises for profit, to any of many other reasons.

As mentioned above PLA collection efforts in the field are very freewheeling and unstructured. But in cyber activities the PRC has adopted a Russian paranoid "cold war mentality." They appear to be trying to keep their cyber war fighters in a rigid military chain of command. In fact there are significant criminal penalties in China for violating cyber restrictions put in place to keep their citizens from freely playing on the web and also acquiring information. The leadership of China is trying to constrain and contain the growing World Wide Web sharing of information. It will be interesting to see if overtime the PRC is capable of stopping their citizen's nascent "Jasmine Revolution" which is currently originating in Africa and the Middle East and spreading.

The PRC essentially has two cyber targets, those external to China and also their own citizens. Only totalitarian dictatorships and closed societies have this challenge. It is an intel/cyber seam for a free and open society to exploit.

But currently today, regardless of internal PRC cyber issues their external attacks continue to be relentless. It is an ongoing struggle by the DOD CI community (NCIS, OSI, Army G-2), NSA, DNI, Law Enforcement (FBI and others) and Homeland Security

to try and stay ahead of this dynamic and significant threat. Several important recent examples of PLA "cyber attacks" have been:

US Naval War College --In December 2006, the Naval War College in Rhode Island had to take all of its computer systems off line for weeks following a major cyber attack. One professor at the school told his students that the Chinese had brought down the system. The Naval War College is where much military strategy against China is developed.

Lockheed Martin's F-35 program --In April, 2009, the Wall Street Journal reported that China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program, the most advanced airplane ever designed. Multiple infiltrations of the F-35 program apparently went on for years.

Two Case Studies-
First case is the Varyag Aircraft Carrier, a study in successful PRC Denial and Deception (D&D)

The Soviet Union was building an aircraft carrier when the wall fell and they went into the dust bin of history. Consequently they put the unfinished carrier up for sale. It was bought by Chong Lot Travel Agency for $ 20 Million US to be used as a floating hotel and gambling parlor. Or so the cover story went. But this turned out to be a huge lie.

The ship was towed from the Black Sea to a Chinese ship yard, and just last week the New York Times announced *"Chinese War Ship May Be Nearly Ready:"*

- *Xinhua's headline with the photos said: "Huge warship on the verge of setting out, fulfilling China's 70-year aircraft carrier dreams"*

It now appears that the PRC denial and deception move was hugely successful.

However, in my professional judgement denial and deception only goes so far against the US Navy/Marine/Air Force Team. Attack submarines, B-2s and USN Carrier Battle Groups like the USS Nimitz Battle Group, named after our Fleet Admiral that presided over the "Miracle At Midway" and victory at sea in WW II, are battle tested.

So if one day the Peoples Liberation Army Navy wants to challenge the American Navy in combat the US will sink their dream carrier the "Shi Lang," named after their Ming Dynasty admiral, any time any place.

The second caseis that of the "Iraq Technology Transfer List" project, (shipping bad things to bad people)

The Chinese have a history of exporting weapons. It is important to note that when dealing with PRC espionage there is a double bounce, first into the PRC and then to other countries. This was seen, as mentioned, with Iran and North Korea but also with Iraq.

Not only is the PLA focused on collecting high tech military and duel use items, they have a vibrant weapons industry and do not hesitate to proliferate anything they have. Especially if the money is right.

The PLA armed Saddam's Military through weapon shipments to Iraq in violation of UN Sanctions. The PRC was second only to Russia on arming Iraq.

In December 2003 I was sent through out Iraq to inventory the conventional contraband weapons shipped to Saddam Hussein in violation of arms embargoes. The weapon smuggling effort was initiated under the provisions of the "oil-for-food" program managed by the French Bank PNB Paribas. The objective of my task was to assess "ground truth" from items found in Iraq in order to identify and bring to justice those individuals and criminal syndicates that had violated UN sanctions.

Support was provided to my mission by those in charge of captured enemy ammunition and unexploded ordnance (CEA/UXO) cleanup. The Army Corps of Engineers and 101st Airborne Division personnel who provided the data that were available.

Countries ranked in violation of arms embargo to Iraq:
U.S.S.R. 122 different types of munitions, total number 12,878,291
China 19 different types of munitions, total number 377,885

Chinese origin of contraband munitions found throughout Iraq by December 2003:

NOMENCLATURE	MODEL
75/40MM	RP TYPE 40
82MM	MORTAR,ILLUM
120MM	MORTAR, HE TYPE 55
122MM	HE TYPE 54
100MM	HEAT TYPE 73
130MM	ILLUM, PROJECTILE TYPE 59,
152MM	HE TYPE 66
152MM	INCENDIARY TYPE 66
GRENADE	RIFLE TYPE 84
GRENADE	HAND, FRAG TYPE 82-1
GRENADE	HAND, FRAG TYPE 86P
HEAT-T	RPG TYPE II
GRENADE	75-MM, HE-T,
ROCKET	107-MM, HE-FRAG, SPINSTABLIZED
ROCKET	SP, 122-MM, HE TYPE 81
107MM	RKT HE Model Ukn
130MM	WARHEAD Type 63
ZH0L LANDMINE	APERS TYPE 72,72B AND72C
LANDMINE	AT TYPE
LANDMINE	APERS, CLAYMORE TYPE 66
FUZE	PROJECTILE, PDSD ML-1

Now to focus on the more high tech UN sanction busting to Iraq---the Asian Wall Street Journal nailed it on the actions of the PRC/PLA firm Huawei:

Technology Two-Timing (March 19 2001):

U.S. intelligence sources confirm (despite a denial from the Chinese government) that Huawei Technologies, one of China's leading makers of communication networks, has helped Iraq outfit its air defenses with fiber optic equipment. The assistance was not approved by the United Nations, and thus violates the international embargo against Iraq. Unless Huawei leaves Iraq and takes its equipment with it, the United States should force American companies to cut Huawei's technology lifeline.

As mentioned above, I investigated criminal syndicates that violated UN sanctions. After the US Coalition Provisional Authority (CPA) was established in 2004 it was apparent that Huawei was bribing their way back into Iraq. It was a simple case they were not allowed in, yet their website in 2004 was bragging about their then current Iraq activities.

Huawei in my professional judgement is an ongoing criminal enterprise using denial and deception techniques and a lot of money and influence to infiltrate their high-tech products into American communication networks.

The Way Ahead- The US has not been ignoring the threat!

In 2007 Justice Department and Partner Agencies launched a national counter-proliferation initiative. (www.justice.gov/opa/pr/2007/October/07_nsd_806.html)

- *WASHINGTON—The Justice Department and several partner agencies today launched a national initiative that will harness the counter-proliferation assets of U.S. law enforcement, licensing, and intelligence agencies to combat the growing national security threat posed by illegal exports of restricted U.S. military and dual-use technology to foreign nations and terrorist organizations.*

- *China and Iran pose particular U.S. export control concerns. The majority of U.S. criminal export prosecutions in recent years have involved restricted U.S. technology bound for these nations as opposed to others.*

Several examples of success -from DOJ press release can be found at justice.gov/opa/pr/2008/October/08-nsd-959.html

Carbon-Fiber Material with Rocket & Spacecraft Applications to China On Oct. 28, 2008, a grand jury in the District of Minnesota returned an indictment charging Jian Wei Deng, Kok Tong Lim, and Ping Cheng with conspiring to illegally export to the People's Republic of China (PRC) controlled carbon-fiber material with applications in aircraft, rockets, spacecraft, and uranium enrichment process.

Space Launch Technical Data and Services to China On Sept. 24, 2008, Shu Quan-Sheng, a native of China, naturalized U.S. citizen and PhD physicist, was arrested in the

Eastern District of Virginia on charges of illegally exporting space launch technical data and services to the People's Republic of China (PRC) and offering bribes to Chinese government officials. Shu was the President, Secretary and Treasurer of AMAC International, a high-tech company located in Newport News, Va., and with an office in Beijing, China.

Electronics & IED Components to Iran – On Sept. 18, 2008, a 13-count indictment was unsealed in the Southern District of Florida charging eight individuals and eight companies with conspiracy, violations of the International Emergency Economic Powers Act, the U.S. Iran embargo, and false statements in connection with their participation in conspiracies to illegally export electronics, Global Positioning Systems (GPS) systems, and other dual-use commodities to Iran. All the items had potential military applications, including in the construction of Improvised Explosive Devices (IEDs).

Avoiding a Black Swan, the impact of the highly improbable Cyber event
(see book by Dr Nassim Nicholas Taleb)

Secretary of the Air Force Mike Wynne's vision, professional experiences and lifelong dedication to American National Security gave him the insight to create the USAF Cyber Command.

That effort was stopped by internal Department of Defense politics. But Secretary Wynne was right about the need and soon a DOD Cyber Command (USCYBERCOM) was created. The USCY BERCOM was enacted into law with a very important mission.
In May 2010, General Keith Alexander first Commanding General outlined his views in his testimony to an Armed Services subcommittee

> *My own view is that the only way to counteract both criminal and espionage activity online is to be proactive. If the U.S. is taking a formal approach to this, then that has to be a good thing. The Chinese are viewed as the source of great many attacks on western infrastructure and just recently, the U.S. If that is determined to be an organized attack, I would want to go and take down the source of those attacks. The only problem is that the Internet, by its very nature, has no borders and if the U.S. takes on the mantle of the world's police; that might not go down so well.*

CONCLUSION

For several years CI representatives working together in NCIX/FBI executive committee sessions have tried to address the extremely hard problem of adjudicating the correct allocation of US Counterintelligence Assets. This is an extremely complex challenge.

Collectors and agents of influence from the PRC can go after objectives many ways as I have discussed. But beyond the scope of my paper they can also buy their way into America through acquisitions and joint ventures-the money offered in those deals is huge.

With respect to PLA cyber espionage efforts to make the situation even more difficult, I believe PRC cyber efforts also have two components: cyber intrusions as collectors and cyber components and software as physical properties. One of the hardest challenges we have faced is defending against cyber collectors and those with malicious intent originating half a world away. Concurrently, the PRC is also trying to place physically compromised components in computers and transmission modalities.

Finally, one must never forget that the human element is always critical—think Private Manning and wikileaks.

If one tries to protect everything because of resource constraints it might wind up that nothing is protected. The most important resource we all need to protect is "time." The hardest resource to allocate in protecting against espionage is the "time" of the CI FBI Special Agents and their fellow Agents in the DOD CI community. The time of those units of Special Agents in the field working cases and also behind computer consuls as cyber defenders, is our most precious and invaluable asset. But I am always optimistic that eventually America will get it right.

Mr. ROHRABACHER. Thank you very much for your testimony. And now Dr. Segal.

STATEMENT OF ADAM SEGAL, PH.D., SENIOR FELLOW, COUNCIL ON FOREIGN RELATIONS

Mr. SEGAL. Mr. chairman and members of the committee, thank you very much for asking me to testify on this very important subject.

I would like to place cyber-espionage in a larger context, which is a push on the Chinese for extremely techno-nationalist technology policy driven toward reducing dependence on advanced countries for foreign technology, and particularly reducing dependence on the United States and Japan. That policy was enshrined in the 2006 Medium-to Long-Term Science and Technology Development Plan, introduced the idea of "indigenous innovation," and it set the goal for China to become an innovated-oriented society by 2020 and among the world's scientific and technology leaders by 2050.

The pursuit of these goals follows three tracks. The first track is industrial policy, which is basically a top-down, state-led focus on big science, but also includes the use of standards policy, the use of procurement and the failure to protect intellectual property rights, as well as forcing technology transfer between foreign companies that want access to the Chinese domestic market.

The second strand is what you would call innovation strategy, and this is a much more market-oriented focus on creating technological entrepreneurship and new growth in the Chinese economy.

And the third strand is cyber-espionage and traditional espionage.

These three strands clearly are overlapped and intertwined, although plucking out the individual strands is difficult to do. In some cases it's very easy. We can see private companies as they grow larger begin to accept funding and support from the state. And also in the case of cyber-espionage as the "Shadows in the Cloud" report shows that there is a nexus between criminal and

state hackers and the information that those hackers find sometimes shows up on the black market and other times it seems to work its way back to state institutions.

The question for the United States, of course, is how do you respond to this? And I think the most important response is domestically: How do we defend our own networks? How do we move to risk management? Because I think most of this is in the end is going to be very difficult to protect, and so we have to think about what type of information we actually want to be digitalized and placed on networks. But also, how do we raise the cost for Chinese hackers, and that's probably going to involve some forms of active defense.

But I think the larger issue as well is: What are U.S. companies saying about this problem? Because like with intellectual property rights theft, U.S. companies do not like to talk about when they have been hacked. We saw with the Google hack, Google said 30 other companies were attacked in this hacking, but then no other company publicly stated that, yes, this was a problem for us. And I think the reasons that they do not state it is because they are afraid of retribution from the Chinese Government. So the United States has to figure out how are you going to respond to that problem and get U.S. Government more involved.

And then the third area, I think, is how do we shape this debate within China. Because we can see with the technology policy there is, in fact, people who question the wisdom of this—excuse me this technology policy, this top-down state strategy. They think that that is not going to be successful long-term and they are afraid that in fact China will fall further and further behind. That Chinese standards will only cut them off from the rest world.

And as Chinese technology companies themselves become more global, they have a stake in a digital infrastructure that is more open and more global. So what the United States wants to do is to think about how we strengthen those individual units.

I suspect, although I have no evidence, that those same factions, we can call them the innovation strategy factions, are also suspicious of a technology policy that is based on espionage. Copying is not going to create incentives for innovation. So those people are the ones that we want strengthen, those are the ones we want to convince that they have an interest in these global structures and these open infrastructures, and to convince them that China is increasingly becoming more vulnerable to cyber-attacks itself.

This is not going to be easy. The techno-nationalist view is widespread in China. It is, in fact, held by the innovation strategy faction. They also want to reduce dependence on the West, but they at least are pushing in more open ways of doing it. So that I think it is important to engage the Chinese on that front, but the more important short-term is probably going to be defending ourselves and raising costs to Chinese hackers.

I'll stop there.

[The prepared statement of Mr. Segal follows:]

COUNCIL on FOREIGN RELATIONS

April 15, 2011

Innovation, Espionage, and Chinese Technology Policy

Prepared statement by
Adam Segal
Ira A. Lipman Senior Fellow for Counterterrorism and National Security
Council on Foreign Relations

Before the
House Foreign Affairs Subcommittee on Oversight and Investigations
United States House of Representatives
1st Session, *112*th Congress

Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology

Chairman Rohrabacher, Ranking Member Carnahan, and members of the committee, thank you for the opportunity to testify on this important subject.

Chinese cyber espionage has to be understood within the context of China's desire to reduce its dependence on the West for advanced technologies, and on the United States and Japan in particular. This goal is laid out in the 2006 National Medium- and Long-Term Plan for the Development of Science and Technology (MLP) which introduced the need for "indigenous innovation" (*zizhu chuangxin*) to lessen the "degree of dependence on technology from other countries to 30 percent or less," (down from 50 percent today, as measured by the spending on technology imports as a share of the sum of domestic R&D funding plus technology imports).[1] Moving from "made in China" to "innovated in China" is essential to the country's future; "Facts tell us that we cannot buy true core technologies in key fields that affect the lifeblood of the national economy and national security," states the MLP. China will become an "innovation oriented society" by 2020 and a world leader in science and technology (S&T) by 2050.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained herein are the sole responsibility of the author.

In pursuit of these goals, China has followed three, often intertwined, tracks: industrial policy, innovation strategy, and cyber and industrial espionage. Industrial policy involves top-down, state-directed technology programs often focused on specific sectors and the government research institutes. The MLP, for example, includes twenty science and engineering megaprojects in such areas as high-end generic chips, manned aerospace and moon exploration, developmental biology, and nanotechnology.

In order to promote indigenous innovation, Chinese policy makers have also used government procurement, developed competing technology standards, and required technology transfer from multinational corporations in return for market access. In 2009, for example, China announced that companies would have to demonstrate that their products included indigenous innovation and were free of foreign intellectual property if they wanted to be a recognized vendor in the government's procurement catalog. In April 2010, Beijing ordered high-tech companies to turn over the encryption codes to their smart cards, Internet routers, and other technology products in order to be included in the catalog.[2] The Chinese have been especially active on the standards front, developing new standards for third generation cellphones (TD-SCDMA), WiFi (WAPI, or WLAN Authentication and Privacy Infrastructure), DVDs (AVS, the audio video coding standard), RFID (Radio Frequency Identification), and other technologies.

The failure to protect intellectual property rights in the Chinese market leads to massive theft and piracy, and in turn improves the short-term competitiveness of Chinese firms. As Senior Director for Greater China at the U.S. Chamber of Commerce Jeremie Waterman said when he testified before the International Trade Commission, a weak legal environment allows Beijing to "intervene in the market for IP [intellectual property] and help its own companies 're-innovate' competing IPR as a substitute to foreign technologies."[3]

In contrast to these state-led efforts, innovation strategy is a more bottom-up, multifaceted effort to create a business environment supportive of innovation and entrepreneurship. These strategies are more dependent on the free market and private entrepreneurship. Often drawing on the experience of Silicon Valley and Route 128 in Boston, these policies focus on small start-ups, university-industry collaboration, and venture capital.

The last strand is the theft of intellectual property either through cyber espionage or more traditional industrial espionage. Since January 2010, Google, Nasdaq, DuPont, Johnson & Johnson, General Electric, RSA, and at least a dozen others have had proprietary information stolen by hackers, although how many of these attacks originated from China is uncertain.[4] Attacks are becoming more sophisticated and increasingly rely on spear phishing (targeted attacks that rely on publicly available information) and other social engineering techniques. In the physical world, Chinese nationals have been recently charged in the theft of radiation-hardened microchips and precision navigation devices.

These three tracks often overlap, in some places more clearly and in others more speculatively. It is not uncommon for a small private firm to attract government attention as it becomes successful. So, for example, a firm founded by a professor who wanted to commercialize research findings would move from the realm of innovation strategy to industrial policy as the company turned to the State High Technology Development Plan (also known as the 863 Program) for investment.

2.

The relationship between technology development policies and espionage, while certainly present, is more difficult to draw out. The government has actively encouraged Chinese nationals working in science and technology fields in the United States and other advanced economies to return home through programs such as the national One Thousand Talents Scheme, Shanghai's Gathering Ten Thousand Overseas Students Project, and the various Overseas Students Parks dotted across the country. These "talents" are offered access to investment capital, subsidized real estate and other preferential policies when they return to Shanghai, Beijing, and other technology centers. In some instances, according to a *New York Times* report, Chinese nationals have applied for government funding to help develop technologies that were stolen from American companies.[5]

The relationship between the state and hackers is even murkier. As the "Shadows in the Clouds" report on computer exploitation notes, there is an emerging ecosystem of crime and espionage. Espionage networks adopt criminal techniques and networks "both to distance themselves from attribution and strategically cultivate a climate of uncertainty." Some of the information stolen by the hackers ends up on the black market, some of it, according to the report, ends up in the "possession of some entity of the Chinese government."[6] At the very least, much of the hacking is state tolerated, in many instances it is encouraged, and in some cases of espionage, it is directed by state actors.

U.S. Policy Responses

It is clear that the United States must do more to defend itself. In the September 2010 issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn III argued that though the "threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyber threat that the United States will face over the long term."[7]

There is, however, an emerging debate whether the traditional methods of cybersecurity—public-private partnerships and information sharing—are adequate to the threat. Given the attacks on Google and other technology companies, there is a real question whether the private sector can defend itself against state-backed attacks. Under these conditions, some have suggested extending the Defense Industrial Base Information Sharing Environment, a forum in which forty defense contractors share information on attacks in return for DOD assistance with network defense, to critical private sector firms. At the very least, private companies must get used to the idea that any information that is digitalized cannot be made completely secure. In this environment, the objective for the private sector is risk management, with the government and U.S. Cyber Command playing defensive and deterrent roles, respectively.

The other policy focus must be an attempt to change Chinese actions and incentives. Efforts to raise the issue of cyber espionage directly with Chinese policy makers have generally elicited two responses. Officials often have a Captain Renault-like response that Beijing is "shocked, shocked" that anything like illegal computer access could happen since hacking is illegal in China. Or they complain, with some justification, that China is itself victim to many cyber attacks, many of them originating in the United States. *The People's Daily*, for example, cites a 2006 report that the approximately 27,000 Trojan horse attacks on China came mainly from the United States.[8] The recent announcement that the FBI is sending a cyber security expert to cooperate with Chinese authorities on investigations is an important first step but to building some trust between the two sides on criminal hacking.

3

American technology companies need to be more vocal about the theft of their intellectual property. While U.S. trade officials often want to press their Chinese counterparts, they are often frustrated with the attitude of U.S. businesses operating in China. American companies complain about the high rates of piracy, but in any intellectual property rights case against China, no one wants to be named as the complainant. Few companies want to alienate the central government in Beijing, and many fear reprisal from local government officials, who levy fines for spurious safety and labor violations, refuse new building permits, or subsidize their competitors.[9]

The same issue is partly at play with computer intrusions. Right now, the majority of companies do not seem interested in knowing more about attacks because of cost and liability issues. According to a recent study by McAfee and SAIC, more than half of 1,000 companies surveyed in the United States, Britain and other countries did not investigate security breaches because of the cost.[10] But it can also be assumed that many do not publicize attacks for fear of alienating the Chinese government. When Google announced in January 2010 that it been undergoing a series of attacks that seemed to be coming from China, it also stated that those same attacks affected thirty other technology companies. Yet after the announcement, no other company admitted to being victim.

While few companies have the ability to leave the China market like Google did, there is evidence that vocal complaints and unified pressure can have some influence on Chinese policy makers, especially since China still depends on foreign companies for access to critical technologies. In the case of WAPI, the competing standard to WiFi, foreign companies refused to go along with requirements to transfer technology to Chinese companies and threatened not to sell wireless chips into the Chinese market. The U.S. government also got involved, with a letter, signed by Secretary of State Colin Powell, Commerce Secretary Don Evans, and U.S. Trade Representative Robert Zoellick that implicitly threatened to pursue the case at the World Trade Organization. Eventually the Chinese government backed down.

The other policy question is: can the United States appeal to those who want China to become more innovative but think industrial policy and indigenous innovation in particular are counterproductive? There are parts of the Chinese bureaucracy promoting innovation strategy; they advocate raising the country's technological capabilities through trade-friendly policies, such as providing greater transparency and enforcing IPR-protection regulations. They have not forgotten that China has benefited immensely from access to billions of dollars in foreign investment, global customers and distribution networks, and technology transfers from American, Japanese, and European firms. In addition, as more Chinese firms expand abroad, they are beginning to realize that their global competitiveness will be severely limited if the Chinese market is isolated as a result of indigenous innovation initiatives.

This "innovation strategy" faction should be sympathetic to similar arguments about the deleterious effects of cyber espionage on Chinese innovation capabilities. In fact, dependence on foreign secrets is likely to lessen the ability (and desire) of Chinese firms to push the technological envelope. The challenge for the United States is identifying and supporting those elements, though how capable they are in fighting against those interests promoting industrial policy and supporting cyber espionage is an open question.

4

Because China's leadership is broadly committed to the goals of reducing dependence on foreign technology any progress on either the industrial policy or cyber espionage front is bound to be slow and uneven. The United States should continue to try and shape the debate within China, but the most important actions will be improving the defense of its computer networks and intellectual property.

I thank the Committee for the opportunity to testify and will be happy to take any questions.

5

[1] "The National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)," State Council, People's Republic of China.

[2] Adam Segal, "China's Innovation Wall: Beijing's Push for Homegrown Technology," *Foreign Affairs*, September 28, 2010, http://www.foreignaffairs.com/articles/66753/adam-segal/chinas-innovation-wall

[3] Testimony of Jeremie Waterman before the US International Trade Commission on "China, Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the US Economy," June 15, 2010, http://www.itcblog.com/wp-content/uploads/2010/06/watermancomments.pdf

[4] "Significant Cyber events since 2006," Center for Strategic and International Studies, Last Modified March 9, 2011, http://csis.org/files/publication/110309_Significant_Cyber_Incidents_Since_2006.pdf; Michael Riley and Sara Forden, "Hacking of DuPont, J&J, GE Were Google-Type Attacks That Weren't Disclosed," *Bloomberg*, March 8, 2011,

[5] Christopher Drew, "New Spy Game: Firms' Secrets Sold Overseas, *The New York Times*, October 17, 2010

[6] Shadows in the Cloud: Investigating Cyber Espionage 2.0," Joint Report, Information Warfare Monitor, Shadowserver Foundation, April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

[7] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[8] America's Two-Faced Tricks Once Again Give It a Lead," translated from the Chinese "美国的两面手法又给自己当头一棒," *The People's Daily*, March 30, 2011, http://opinion.people.com.cn/GB/14278366.html

[9] Adam Segal, *Advantage: How American Innovation Can Overcome the Asian Challenge*, W. W. Norton and Co., January 10, 2011

[10] Brian Grow, "Special Report: In Cyberspy vs. Cyberspy, China has the Edge," *Reuters*, April 14, 2011, http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414

Mr. ROHRABACHER. Thank you very much.

And Mr. Carnahan may not be able to join us after the next series of votes, so I think we will give you the courtesy of asking your questions now.

Mr. CARNAHAN. Great. Thank you, Mr. Chairman. And thanks to all the panels here today. This has been a very good overview.

I wanted to start with just an overall question to really any of the panelists that want to weigh in on this. President Obama had stated that "our ability to partner is a prerequisite for progress on many of the most pressing global challenges." I wanted to get your assessment of the willingness of the Chinese to engaged with the U.S. in this manner regarding cyber threats and technology threats. And why do we not just start with Mr. Choate and work our way across?

Mr. CHOATE. Well, I think we can anticipate—well I think I can start by looking at our own history. From 1790 to around 1838 the United States was under a very aggressive policy of technology acquisition under a manufacturing strategy put together by Alexander Hamilton. We literally stole everything that we could from any place in the world.

And I think that China, and any other developing country, would feel an obligation to do almost the same thing. From our perspective I think we must assume that for years to come as long as our technology is superior, they have ever incentive in the world to go out and steal our technology. That gives a series of mandates on what we should do as a country.

We should be not naive. We should take a look at the way that we have agglomerated technology, who has access to it, how we in effect have our companies understand that one of the things they've got do is take certain of their computers off of the internet. We need to take a look at our policies with the Patent Office with all of the new technologies there. In other words, we must assume as a policy that not only China, but Germany and Brazil and other countries are out to steal to our technology. It's our responsibility to not make it easy as we do now.

Mr. CARNAHAN. And before I get to the next witness, to the extent that China is becoming a target increasingly of intellectual property——

Mr. CHOATE. Yes.

Mr. CARNAHAN [continuing]. Is that going to get them to the table on these issues?

Mr. CHOATE. Not really, I don't think so.

One of the things that is happening with the Chinese, they have made in their last 5-year plan a major effort to do patenting in China. Probably the largest set of patenting in the world now is done inside China. So their conscious about the need to create legal rights and at the same time they're conscious about securing their own technology. So I do not think that we're really going to wind up with any real cooperations. I think we must proceed on that basis.

Mr. CARNAHAN. Thank you. I am going to try to get everybody in if we can after this bell went off.

Mr. Fisher?

Mr. FISHER. Thank you, Mr. Chairman.

I do not see that the Chinese Government today shares any interest in partnering with the United States in an effective way, at least as we would view it. The cyber warfare effort along with the range of miliary modernization efforts that we have seen underway all date back to the 1989 Tiananmen uprising. That scared the bejesus out of the Chinese Communist leadership. And all that they have done since then in the military strategic sphere has been devoted to protecting their dictatorship, their control, their position of power to include this aggressive campaign of cyber warfare.

They are not going to be interested in talking to us until they have reached a level of power for which they are comfortable. And I am not sure that their concepts of partnering will include any kind of concept of equality that we have, that we will share interests and then move forward. Once they gain a position of superiority, they are going to want to start dictating and changing the rules, rewriting rules.

Mr. CARNAHAN. Let me move on to Mr. Timperlake.

Mr. TIMPERLAKE. Yes, sir. Thank you for the question.

I think you have to approach it from two perspectives. The first is they are very good at denial and deception, which is their charm offensive. They will stay engaged and do whatever accrues to their advantage. No problem, no debate on that. What they will do, though, is take it to their advantage first and foremost through their 16 character policy. Where I think you can actually find their true intentions is if you read their War College literature. Surprisingly, or not surprising, the Chinese will tell you, the PLA, what their intentions are. In fact, they are quite proud of what they are doing.

So the engagement policy always has to go in with that huge caveat that they are very, very good, as you saw, taking an aircraft carrier and calling it a casino, and then converting it into a ship of war. So when you engage at that level be careful.

Mr. CARNAHAN. Mr. Segal?

Mr. SEGAL. I do not fundamentally disagree with most of the bad news that the panelists have given you, but I will try to give a glimmer of hope here.

On one hand, I think there are some parts of the Chinese bureaucracy that are beginning to think about how they defend themselves from these vulnerabilities. We see a track now that is going on with some members of the Ministry of State Security and MIIT that are participating on these discussions.

At the U.N. the Chinese have unwillingly gone along with the Russians for discussions about cyberspace arms control agreements.

And in my own dealings with members of the Ministries, they are beginning to practice certain arguments, rule them out about how they want to engage in cyberspace.

I think it is very early. I am not expecting any progress on those fronts, but I think within the Chinese bureaucracy there is some thinking about it. But I do not widely disagree with the generally negative that the panel has given.

Mr. CARNAHAN. Great. Thanks to all of you.

Thank you, Mr. Chairman., Yield back.

Mr. ROHRABACHER. Thank you.

How many minutes do we have? We have 10 more minutes to get to the vote, and I think what I am going to do is get my questions now and seeing that our other members are not here, that will be the end of the hearing. So, we do have 10 minutes.

So if you would like to any moment, because we are restricted here, you can jump in and ask a follow-up question as well, Mr. Carnahan.

What about joint ventures with Chinese companies? We have aerospace industry and others who are pushing in that area. Is this going to work for us or against us? And be succinct and we will go on down?

Mr. CHOATE. Basically what we are doing is giving away our technology.

Mr. ROHRABACHER. And so the things that we have developed and spent billions of dollars developing will then be eventually used competitively against us?

Mr. CHOATE. Yes.

Mr. ROHRABACHER. Mr. Fisher?

Mr. FISHER. Absolutely, I agree with Pat on this.

We are helping the Chinese to build competitors to Boeing and Airbus, and that advantage will be much narrower by the end of this decade. And the Chinese are taking all of this technology and applying it to military programs that will be largely aimed at us as well.

Mr. ROHRABACHER. This policy has destroyed several manufacturing industries in the United States already. And for us to put at risk the aerospace industry with this type of involvement, would the Chinese who are clearly our adversaries, certainly more than just our competitors but our adversaries and perhaps our enemies? Mr. Timperlake?

Mr. TIMPERLAKE. Yes, sir, I think you are exactly right. In fact, one dimension of the role out of the J–20 that catches my interest is they are notorious proliferators. So in addition to perfecting a fifth generation aircraft, you can expect them to try and sell a fifth generation aircraft. And that will intrude on the international aircraft market to their benefit. So they steal stuff, they build something and they proliferate it and they do it for money, or they will buy their way in. And they are very good at that.

Mr. ROHRABACHER. Mr. Segal?

Mr. SEGAL. Clearly in aerospace and avionics the joint ventures are probably not going to be good for U.S. national or economic security interests. But I think in a range of other economic sectors companies have moved away from the joint venture model because of the technology transfer reason. They have moved to wholly foreign-owned ventures and not wanting to partner for this technology transfer reason. And they themselves have become gradually over time more sophisticated in breaking up technology into specific components and making sure that the most advanced components do not go into China. But I think for national security reasons there are certain sectors that do.

Mr. ROHRABACHER. Of course, it is not necessarily what goes into China physically, but——

Mr. SEGAL. Yes.

Mr. ROHRABACHER [continuing]. Perhaps what the Chinese can hack into and bring the plans over.

Mr. Fisher, you had something you wanted to add?

Mr. FISHER. ...is important as well, because in my opinion, at least what some Chinese sources have told me, they have their own F–35 program as well. A lower cost fighter, fifth generation fighter that, as Mr. Timperlake mentioned, will be on the market probably within the decade.

Mr. ROHRABACHER. And is that based on our research and development, Mr. Timperlake?

Mr. TIMPERLAKE. It is an important point. What I found in my research is that the Chinese acquisition system which we still are trying to figure out, we have trouble with our own of course, is develop, develop, steal, develop, steal, buy, develop; whatever. But what happens is they go dark for a period 5 to 7 years so they can surprise you.

And if they laid out the J–20 as more a surprise then anything, what is next, and what is next is cascading in from the great spy cases of the '90s and those cyber intrusion to this day. So, there are surprises still coming in their perfection of technology.

Mr. ROHRABACHER. We have a major economic challenge before us. And I would suggest that from the testimony we hear today a considerable amount of that challenge can be traced to the fact that we now have permitted in wealth in the form of research and technology development to be stolen or just transferred to a competitor.

Yes, Pat?

Mr. CHOATE. The problem really extends across our advanced technology trades. Department of Commerce does an analysis. We are running an $80-billion-a-year deficit in advanced technology trade. The largest part of that deficit is now with China.

I think that what we have to be leery about is that the Chinese on certain technologies, once they gain control of those, they will use that as they have their control of 90 percent of the world's rare earths as strategic leverage, foreign policy leverage. Our risk is that we become totally dependent upon China or the countries immediately around China, in the China sphere those ten countries for certain of our most vital technologies. And we are well on the way of having such a dependency.

Mr. ROHRABACHER. Well, let me just note that we are going to break in a few minutes. So, I am sorry, I apologize for that but this is the way it has worked out today.

We face many challenges as a free people. One is how are we going to be prosperous and our people are going to have a decent standard of living. And number 2, of course, and which is probably the number one concern, is how are we going to make sure that we are safe from threats to our security and the safety of our people. And in both of these goals that should be primary goals of the Federal Government, the transfer of technology and the cyber theft of American technology is putting our ability to have a prosperous and have a safe American, it is putting that at risk. This is an issue that I am pretty happy this is one of the first things we covered in this subcommittee. We will be coming back to that and probably asking you gentlemen to return in a few months. But we

have broken the ground here. And we want to make sure that we have a national debate on where we draw the line.

I would say the American people would be outraged to understand that tens of billions of dollars that have been taken from them in order for research and development in our country has ended up in the hands of an economic and military adversary like Communist China, which is also one of the world's worst human rights abusers.

So, if we are going to preserve the peace and we are going to have prosperity in America, we have got to come to grips with this challenge.

I have got to come to grips because I have got 3½ minutes left to vote.

I would like to thank you all for testifying.

This hearing is adjourned.

[Whereupon, at 1:01 p.m., the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

Subcommittee on Oversight and Investigations
Dana Rohrabacher (R-CA), Chairman

April 13, 2011

You are respectfully requested to attend an OPEN hearing of the Subcommittee on Oversight and Investigations, to be held in **Room 2172 of the Rayburn House Office Building (and available live, via the WEBCAST link on the Committee website at http://www.hcfa.house.gov):**

DATE: Friday, April 15, 2011

TIME: 12:00 p.m.

SUBJECT: Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology.

WITNESSES: Pat Choate, Ph.D.
Director
Manufacturing Policy Project

Mr. Richard Fisher
Senior Fellow, Asian Military Affairs
International Assessment and Strategy Center

The Honorable Edward Timperlake
(Former Director,
Technology Assessment, International Technology Security,
Office of the Secretary of Defense, U.S. Department of Defense)

Adam Segal, Ph.D.
Senior Fellow
Council on Foreign Relations

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Oversight and Investigations* HEARING

Day *Friday* Date *4-15-2011* Room *2172*

Starting Time *12:10 pm* Ending Time *1:02 pm*

Recesses *n/a* (____ to ____) (____ to ____) (____ to ____) (____ to ____) (____ to ____) (____ to ____)

Presiding Member(s)

Chairman Rohrabacher

Check all of the following that apply:

Open Session ☑
Executive (closed) Session ☐
Televised ☑
Electronically Recorded (taped) ☑
Stenographic Record ☑

TITLE OF HEARING:

Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology

SUBCOMMITTEE MEMBERS PRESENT:

Rep. Rohrabacher, Rep. Carnahan, Rep. Cicilline, and Rep. Bass.

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

none

HEARING WITNESSES: Same as meeting notice attached? Yes ☑ **No** ☐
(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

Pat Choate- Prepared Statement
Richard Fisher- Prepared Statement
Ed Timperlake- Prepared Statement
Adam Segal- Prepared Statement

TIME SCHEDULED TO RECONVENE *Noon*
or
TIME ADJOURNED *1:02 pm*

Subcommittee Staff Director