

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 than 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” than 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 case is 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 dual 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:

<u>NOMENCLATURE</u>	<u>MODEL</u>
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, SPINSTABILIZED
ROCKET	SP, 122-MM, HE TYPE 81
107MM	RKT HE Model Ukn
130MM	WARHEAD Type 63
ZH0L LANDMINE	APERS TYPE 72, 72B AND 72C
LANDMINE	AT TYPE
LANDMINE	APERS, CLAYMORE TYPE 66
FUZE	PROJECTILE, PDS 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 USCYBERCOM 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.

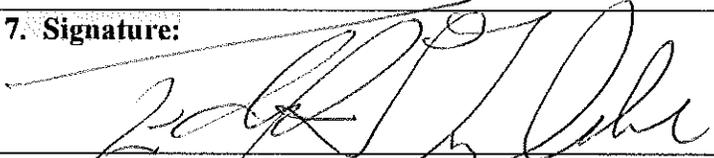
Finally, one must never forget that the human element is always critical—think Private Manning and wikileaks.

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.

United States House of Representatives
Committee on Foreign Affairs

"TRUTH IN TESTIMONY" DISCLOSURE FORM

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

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

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