CHINA'S PROLIFERATION PRACTICES, AND THE DEVELOPMENT OF ITS CYBER AND SPACE WARFARE CAPABILITIES

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

———————

MAY 20, 2008

———————

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION
WASHINGTON : JUNE 2008

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

LARRY M. WORTZEL, *Chairman*
CAROLYN BARTHOLOMEW, *Vice Chairman*

Commissioners:

PETER T.R. BROOKES	Hon. WILLIAM A. REINSCH
DANIEL BLUMENTHAL	Hon. DENNIS C. SHEA
MARK ESPER	DANIEL M. SLANE
JEFFREY FIEDLER	PETER VIDENIEKS
Hon. PATRICK A. MULLOY	MICHAEL R. WESSEL

T. SCOTT BUNTON, *Executive Director*
KATHLEEN J. MICHELS, *Associate Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act for 2001 § 1238, Public Law No. 106-398, 114 STAT. 1654A-334 (2000) (codified at 22 U.S.C.§ 7002 (2001), as amended by the Treasury and General Government Appropriations Act for 2002 § 645 (regarding employment status of staff) & § 648 (regarding changing annual report due date from March to June), Public Law No. 107-67, 115 STAT. 514 (Nov. 12, 2001); as amended by Division P of the "Consolidated Appropriations Resolution, 2003," Pub L. No. 108-7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of Commission); as amended by Public Law No. 109-108 (H.R. 2862) (Nov. 22, 2005) (regarding responsibilities of Commission and applicability of FACA); as amended by Division J of the "Consolidated Appropriations Act, 2008, "Public Law No. 110-161 (December 26, 2007) (regarding responsibilities of the Commission, and changing the Annual Report due date from June to December).

The Commission's full charter is available at www.uscc.gov.

CONTENTS

———

TUESDAY, MAY 20, 2008

CHINA'S PROLIFERATION PRACTICES, AND THE DEVELOPMENT OF ITS CYBER AND SPACE WARFARE CAPABILITIES

PANEL IV: ADMINISTRATION PERSPECTIVES

PANEL V: CHINA'S PROLIFERATION PRACTICES

June 20, 2008

The Honorable ROBERT C. BYRD

President Pro Tempore of the Senate, Washington, D.C. 20510

The Honorable NANCY PELOSI

Speaker of the House of Representatives, Washington, D.C. 20515

DEAR SENATOR BYRD AND SPEAKER PELOSI:

We are pleased to transmit the record of our May 20, 2008 public hearing on *"China's Proliferation Practices and the Development of its Cyber and Space Warfare Capabilities."* The Floyd D. Spence National Defense Authorization Act (amended by Pub. L. No. 109-108, section 635(a)) provides the basis for this hearing.

In this hearing, witnesses told the Commission that while China's proliferation practices have improved, its activities in other areas of national security continue to raise concerns. China is aggressively pursuing a space program that has military applications. China's activities in cyber space also represent a growing challenge to the national and economic security of the United States.

The first panel of the day addressed China's recent advances in outer space and their implications for the United States. The panel featured Brigadier General Jeffrey Horne from the U.S. Strategic Command, Dr. Ashley Tellis from the Carnegie Endowment for International Peace, and Mr. Bill Scott, formerly an *Aviation Week and Space Technology* editor. The panel concluded that China continues to make significant progress in its space capabilities, many of which easily translate to an enhanced military capacity in space. Unlike the United States, the military runs China's space program, and there is no separate, distinguishable civilian program. Although some Chinese space programs have no explicit military intent, many space systems—such as communications, navigation, meteorological, and imagery systems—are dual-use in nature.

While the People's Liberation Army currently has sufficient capability to meet many of its goals of conducting a limited war under modern high-tech conditions, planned expansion in electronic and signals intelligence, in part facilitated by new space-based assets, will provide greatly increased intelligence and targeting capability. These advances will result in an increased challenge to U.S. military assets, thereby increasing the cost to the United States of any future conflict with China.

The second panel addressed the threat that Chinese cyber space operations pose to U.S. national security. This panel featured Colonel Gary McAlum, Director of Operations for the U.S. Strategic Command's Joint Task Force for Global Network Operations; Dr. James Mulvenon, Director of Advanced Studies and Analysis at Defense Group, Incorporated; and Mr. Timothy L. Thomas, a China and cyber security analyst at

the Army's Foreign Military Studies Office at Ft. Leavenworth, Kansas. The panelists agreed that cyber space is a potential critical vulnerability of the U.S. government and economy since both are so dependent on the use of computers, and connections to the Internet make them difficult to secure. China is likely to take advantage of this reality for two significant reasons. First, the costs of cyber operations are low in comparison with traditional espionage or military activities. Second, determining the origin of cyber operations, and attributing them to the Chinese government or any other operator, is difficult. Computer network operations provide a high degree of plausible deniability. The panelists noted that measures soon should be implemented by the United States to help strengthen critical U.S. computer networks against cyber intrusion. However, considerably more work and investment, particularly with respect to privately-owned and operated cyber networks, will be required to provide adequate security for the computer networks on which America depends.

The final two panels examined China's proliferation practices and its nonproliferation policies. Principal Deputy Assistant Secretary of State for International Security and Nonproliferation Patricia McNerney testified that China is a party to many international nonproliferation agreements and regimes and has taken laudable steps to design and implement comprehensive national export control regulations. The United States and China continue to cooperate on export controls through technical exchanges and training. For example, last year the United States held discussions with China North Industries Corporation (NORINCO) and China Great Wall Industries Company (CGWIC)—two companies with long records of proliferation—regarding their commitment to end proliferation-related activity. In addition, Ms. McNerney praised China's support for sanctions in the UN Security Council to pressure Iran and North Korea to curtail their respective suspected nuclear weapons activities. However, Ms. McNerney noted that China "admittedly has not actively cooperated to ensure closure of North Korean front companies inside China that facilitate proliferation, or the Chinese companies that supply them." Furthermore, she testified that "a number of Chinese entities continue to supply items and technologies useful to weapons of mass destruction, their means of delivery, and advanced conventional weapons to countries of concern." Particularly worrisome are transfers of Chinese conventional arms to Iran that have been found among insurgents and militants operating in Iraq against U.S. forces.

Mr. Stephen Rademaker, Senior Counsel at Barbour Griffith and Rogers, LLC and former Assistant Secretary of State for International Security, and Mr. Henry Sokolski, Executive Director of the Nonproliferation Policy Education Center and former Deputy for Nonproliferation Policy in the Office of the Secretary of Defense, followed Ms. McNerney. Mr. Rademaker testified that the willingness of NORINCO to discuss and agree to change its behavior and policy toward proliferation of weapons and technology is the "best advertisement for [the United States'] policy of [imposing] sanctions [on proliferating enterprises]." In addition, Messrs. Rademaker and Sokolski agreed that the imposition by the United States of financial sanctions, such as those imposed in 2005 on Banco Delta Asia in Macau that allegedly served as a channel for financing proliferation activities, provided a useful incentive for China to improve enforcement of its nonproliferation policies and regulations. Mr. Sokolski warned that any changes China

makes to its nuclear policy or any modernization of its nuclear weapons program could spur other Asia Pacific nations to acquire nuclear capability. In order to reduce proliferation risks, he recommended that the United States encourage China to cap its production of nuclear weapons-usable fuels and discourage state-to-state transfers of nuclear weapons in peacetime.

The prepared statements of the hearing witnesses can be found on the Commission's website at www.uscc.gov, and the complete hearing transcript also will be available on the website. Members of the Commission are available to provide more detailed briefings. We hope the information from this hearing will be helpful as the Congress continues its assessment of U.S.-China relations. The Commission will examine in greater depth these issues, and the other issues enumerated in its statutory mandate, in its 2008 Annual Report that will be submitted to Congress in November 2008.

Sincerely yours,

Larry M. Wortzel
Chairman

Carolyn Bartholomew
Vice Chairman

cc: Members of Congress and Congressional Staff

CHINA'S PROLIFERATION PRACTICES

AND THE DEVELOPMENT OF ITS CYBER AND

SPACE WARFARE CAPABILITIES

_____

TUESDAY, MAY 20, 2008

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 562, Dirksen Senate Office Building, Washington, D.C. at 10:05 a.m., Commissioners Peter T.R. Brookes and William A. Reinsch (Hearing Cochairs), presiding.

OPENING STATEMENT OF COMMISSIONER WILLIAM A. REINSCH, HEARING COCHAIR

HEARING COCHAIR REINSCH: The hearing will come to order. Vice Chairman Bartholomew is unable to be with us this morning, so I will read her opening statement and then turn it over to the hearing co-chair, Commissioner Brookes.

Welcome to the fifth hearing of the U.S.-China Economic and Security Review Commission's 2008 reporting cycle. We're pleased that all of you could join us today. At this hearing, we will focus on emerging issues in the U.S.-China security relationship and also review the progress on a past issue in that relationship: proliferation.

Today's panels will assess the impact on U.S. national security of China's space warfare and cyber warfare activities and developments in these areas as well as its proliferation practices and nonproliferation compliance.

Last year's anti-satellite test in January and recurring reports about cyber attacks and hacking of U.S. government computer systems highlight the importance of these issues.

The development of China's cyber and space warfare capabilities presents new challenges for the United States in the defense of our country and the conduct of bilateral relations. Of particular importance is the need for transparency on these issues and for China to articulate more clearly the intentions behind its drive to develop these capabilities.

With regard to proliferation, China has made positive steps to adopt nonproliferation policies and to curb its exports of nuclear and missile technology.

However, in last year's report to Congress, the Commission highlighted concerns about China's implementation and enforcement of its nonproliferation policies and its willingness to support an international effort aimed at preventing Iran and North Korea from further developing a nuclear weapons program.

I look forward to the testimony of our witnesses today who have been asked to speak about China's proliferation practices, nonproliferation compliance and approach to its commitments.

Before I turn the gavel over to Commissioner Brookes, let me also on behalf of the Commission express our condolences to the Chinese people for their losses in the regions struck by the terrible earthquake that they've been experiencing. We wish them well, and we wish them the best in their relief efforts.

Commissioner Brookes.

OPENING STATEMENT OF COMMISSIONER PETER T.R. BROOKES, HEARING COCHAIR

HEARING COCHAIR BROOKES: Thank you. Good morning. I'm Peter Brookes, cochairman of today's hearing along with my colleague Commissioner Bill Reinsch.

Today's hearing concerns itself with China's weapons proliferation practices and its development of cyber warfare and space warfare capability.

I want to first thank the members of Congress who will testify at today's hearing. I also would like to thank Congress for the support and interest so many members have shown for the work of the Commission since it was established eight years ago in 2000 to advise members on national security and economic policy toward China.

Since that time, the Commission has produced five annual reports including recommendations for legislative and policy changes.

Cochairman Reinsch will be chairing the proliferation panel this

afternoon, but let me say a few words on space and cyber warfare, the panels that I will chair.

China's activities in space and cyberspace have been the subject of much discourse in the national security community and the media around the world in recent months. Strikingly, the People's Liberation Army was responsible for an unannounced direct ascent shoot down of one of its own satellites in early 2007. It is also developing its own satellite architecture including navigational intelligence satellites and is likely involved in developing other kinetic and non-kinetic anti-satellite programs.

It was also reportedly behind numerous incidents of cyber intrusion of U.S. government and military computer networks. The same is true of a number of incidents of intrusion against foreign governments, which were widely reported earlier this year.

Industry is also a target of cyber espionage. In a recent private sector report, a well-known computer security company asserted that offensive computer network operations are on the rise worldwide. The report singled out China at the forefront of what some are now calling a new "cyber Cold War."

Although Chinese officials routinely deny involvement in any specific intrusive computer network events, official PLA papers openly state that the Chinese military will continue to pursue the capability to conduct war in cyberspace as part of their overall warfighting doctrine.

Today we'll hear from a variety of witnesses, from inside and outside of government, who will address these very important and timely topics. The Commission will take today's testimony into account when it later formulates its own recommendations to the Congress. We thus appreciate the work that the many distinguished witnesses have put into preparing their statements and their making time in their busy schedules to be here today.

We understand that there may be times when questions posed by the commissioners are better answered in a private setting. The witnesses should be aware they should feel free to tell us when we have reached that threshold.

Once again, thank you all for being here. The Commission will recess until Representative Lofgren joins us or until 10:30 when we'll begin the first panel. Thank you very much.

[Whereupon, a short recess was taken.]

HEARING COCHAIR REINSCH: The hearing will come back to order. Commissioner Brookes.

HEARING COCHAIR BROOKES: Good morning. If the panelists would come to the witness table, please.

We were hoping to have Representative Lofgren address us before we got started this morning. If she does join us, I will interrupt your testimony to allow her to talk to us since she's on a very, very tight schedule. But for the moment, we'll just proceed as normal.

We'd appreciate if you could keep your testimony to seven or so minutes and then we can leave the maximum time for questions and answers. Thank you all for being here.

On this panel this morning, we're going to be talking about China's space capabilities with a particular focus on China's military space program development.

Our first speaker will be Brigadier General Jeffrey C. Horne. He is the Deputy Commander of the Joint Functional Component Command for Space in the United States Strategic Command.

He's also Deputy Director for Mission Support at the National Reconnaissance Office. From July 2004 to January 2006, he was Deputy Commanding General for Operations, U.S. Army Space and Missile Defense Command and United States Army Forces Strategic Command at Peterson Air Force Base in Colorado.

Our second speaker will be Dr. Ashley J. Tellis. He's a Senior Associate at the Carnegie Endowment for International Peace. He specializes in international security, defense, and Asian strategic issues.

He was recently on assignment at the U.S. Department of State as a Senior Adviser to the Undersecretary for Political Affairs, during which time he was involved in negotiating the civil nuclear agreement with India.

Good morning. Come on up here. We'll go ahead and take Representative Lofgren at this time since she's on a busy schedule. Good morning and welcome.

PANEL I: CONGRESSIONAL PERSPECTIVES

STATEMENT OF ZOE LOFGREN
A U.S. REPRESENTATIVE FROM THE STATE OF CALIFORNIA

MS. LOFGREN: Good morning to you. I'm sorry I'm late. That's the state that we find ourselves in these days, and I have a Homeland Security markup in just a short time. I am happy to visit here with some new friends and some old friends, Bill, on this important subject.

HEARING COCHAIR BROOKES: Yes, please proceed.

MS. LOFGREN: As you no doubt know, the state of our security--I'm speaking now on the civilian side primarily--from a cyber security point of view is I think unacceptably low. The Federal

Information Security Management regulations, or FISMA, is our primary bulwark for computer and network security in the federal government.

It's not at all clear to us in Homeland overlooking the various departments that the FISMA standards are even being deployed throughout the federal government, and certainly it's not clear that the FISMA standards provide an adequate level of security from a cyber point of view.

So, we have two problems: one, the standard is too low; and that standard has not been uniformly adhered to throughout the federal government. I do think that's a concern. The subject here, of course, is China, and we do know without getting into anything that we shouldn't talk about in public that China is a great source of hacking and cyber probing. Certainly, China has or at least sites within China have repeatedly intruded into civilian sites.

The Department of Commerce--in October of 2006, hackers operating through Chinese Internet servers, launched an attack on the computer system of the Bureau of Industry and Security. Obviously, we can't be sure that all of the attacks actually originated in China, but they did come through the ISP.

Certainly the State Department has had hacking intrusions with sensitive information and passwords selected from unclassified computer systems. Even though these are not classified systems, and certainly in the appropriate format, you'll get information on classified systems, there's a lot of sensitive information that is available on nonclassified sources.

So given the fact that FISMA has not been uniformly applied and does not provide the level of security we need, in any case, the fact that information is available in an unclassified format, is not properly secured, and has been harvested, if you will, for information I think is cause for concern.

Certainly, all of us know that as the years go by, the value and utility of computer systems and networks becomes more and more important, and as we modernize and utilize these systems, our vulnerabilities also become greater.

I'm not going to talk about the growth of botnets in China and all of the information that is available to you. I'm sure you're well aware of that. I would just like to express a concern that I have expressed repeatedly to management in the Department of Homeland Security, and that is the exposure that the infrastructure of the United States has to cyber attack.

The focus of the federal government most recently under the leadership of the Secretary of Homeland has been to focus on the networks of the federal government itself from--I'm trying to make

sure I don't talk about anything that has been revealed to me in classified briefings, but certainly it's been in the newspaper that the number of portals will be reduced so to enhance the ability to secure the cyber environment in the federal government.

That's all well and good. I have some issues on the deployment and some other things I won't go into, but the fact is that most of the infrastructure of the United States is in the hands of the private sector, and there are substantial vulnerabilities. It's not so much the computer industry that's vulnerable. It's the non-computer industries that in some cases may not have a thorough enough understanding of the vulnerabilities or may not have the incentive, especially where there are interchange sites where nobody has complete responsibility and where the greatest vulnerabilities may lie. Nobody has the complete responsibility to secure those sites.

I'll also say without the risk of being dismissive, and I don't want to be overly dismissive, I think that the Department itself is really not where it needs to be in terms of broad expertise and reputation, if that's a delicate way of putting it, in the area of cyber security, and so I've even thought perhaps many elements of the analysis of our vulnerability at a minimum ought to be provided to Lawrence Livermore Lab or one of the other organizations that really has a greater ability to access expertise in an appropriate and if necessary discrete or classified environment.

That has not yet occurred, but I think as we move forward in a new administration, we very much need to look at how do we develop the expertise that we need, deploy it, not just across the federal government but in a leadership mode with the private sector, so that we can secure the infrastructure of the United States whether it is from Chinese cyber attacks or any other. It really doesn't matter the origin.

I will say that countries that permit or acknowledge or allow the prevalence of cyber attacks I think do put at risk their economic vitality in the world. So any country that would countenance the kind of attacks that we think have emanated from the ISP really should be in a position to rethink that posture because ultimately it will not be to their benefit in a worldwide economic forum. I do think, although there are tensions from time to time with the United States and many other countries around the world, economic ties are those that can help us avoid strong conflict and instead bring us together, and the cyber attacks that occur really are a detriment to that overall goal.

So with that, I have a few minutes before I have to rush to Homeland Security if there are comments, or I also take advice. I can always use it.

Thank you very much.

Panel I: Discussion, Questions and Answers

HEARING COCHAIR BROOKES: Are there any questions for Representative Lofgren?

HEARING COCHAIR REINSCH: I'd just thank you for showing up and for your profoundly rational views, both on this subject and on immigration, another subject close to my own heart.

Can you just say a word, a little bit more, about the reduction in portals issue, which has been in the newspaper? I understand the security advantages of that. Doesn't that create other vulnerabilities, though, if you do that?

MS. LOFGREN: Well, the theory is, I mean you're right. With every step to secure, new vulnerabilities are made available. If, for example, you, let's say, what if that adequate intrusion technology were not--vigorous intrusion technology were not deployed in a ubiquitous manner, the ability to limit the portals so that the full vigorous security were in play would be enhanced.

On the other hand, if inadequate measures are taken, then the vulnerabilities, in fact, are enhanced because you've got no other way. The hackers only have to do maybe five things instead of many others. So you're right. And given where we are in cyber expertise, I think the concern that I think is behind your question is a substantial one.

HEARING COCHAIR BROOKES: Representative Lofgren, you sit on the Homeland Security Committee.

MS. LOFGREN: Yes.

HEARING COCHAIR BROOKES: Where would you rank the cyber threat among the threats of the issues under the jurisdiction of the Homeland Security Committee?

MS. LOFGREN: Let me say that Jim Langevin, who is the chairman of the subcommittee with jurisdiction, has done really a very good job. He's taken this very seriously, spends a lot of time on it, but I will say this, in the 108th Congress, there was a subcommittee that had no jurisdiction other than cyber security. Now, Jim's subcommittee has jurisdiction over cyber, bio, and a whole host of other very important threats. So it's impossible to give, good as he is, and he is very good, to give all the attention to this subject when he has bio threats and other things as well.

I think in terms of our vulnerability, if you could bring down the power grid, for example, you would do substantial damage to the United States. If you could remotely impact other utilities or financial services, that the potential for damage to the economy and to the security of the nation is very high and should not be understated.

HEARING COCHAIR BROOKES: Do you have time for one more question?

MS. LOFGREN: Yes.

HEARING COCHAIR BROOKES: Commissioner Mulloy.

COMMISSIONER MULLOY: Congresswoman, you talked about the worry about the intrusion into our society and the economic damage that could be done. Has there been any discussion within the Congress about maybe trying to get an international treaty that we would all sign to legally bind ourselves not to be doing these kinds of intrusive interventions into one another's societies? MS. LOFGREN: As you know, Congress doesn't get to negotiate the treaties. But there hasn't been a lot of discussion that I'm aware of on this subject nor has any of the trade deals that we, the Congress, does have to approve included this. I do think it's a proper subject for discussion among nations, and I hope that as we move forward that that will be a discussion.

COMMISSIONER MULLOY: Thank you, Congresswoman.

MS. LOFGREN: Thank you very much.

HEARING COCHAIR BROOKES: Thank you for being here.

Just so everybody knows, that was Representative Lofgren from the 16th District of California. She was first elected in 1994 and serves on four committees--Judiciary, Homeland Security, House Administration, and Joint Committee on the Library. She chairs the House Judiciary Subcommittee on Immigration, Citizenship, Refugees, Border Security and International Law.

We appreciate her being here with us today and for sharing her thoughts on these very important issues.

PANEL II: PRC SPACE CAPABILITIES

Let me get back to the second panel. Our third witness will be Mr. William B. Scott. He's an author and former editor of Aviation Week and Space Technology and has 22 years working with Aviation Week. He also served as Senior National Editor in Washington in Avionics and Senior Engineering Editor positions in Los Angeles.

He's a flight test engineer, graduate of the U.S. Air Force Test Pilot School, and a licensed commercial pilot with instrument and multi-engine ratings.

Thank you all for being with us today. We look forward to your testimony. General, if you would start, that would be great.

STATEMENT OF BRIGADIER GENERAL JEFFREY C. HORNE DEPUTY COMMANDER, JOINT FUNCTIONAL COMPONENT COMMAND FOR SPACE, U.S. STRATEGIC COMMAND VANDENBERG AIR FORCE BASE, CALIFORNIA

BRIGADIER GENERAL HORNE: Sure. Well, thank you very much for inviting us here today, Mr. Chairman and all the distinguished members of the Commission. This is my first opportunity to talk to you and I certainly appreciate it.

I believe that this Commission fills a very important role in advising Congress in our country's relationship with the People's Republic of China, and I appreciate the opportunity to share with you the views of General Kevin Chilton, Commander of U.S. Strategic Command (USSTRATCOM) and my boss, Lieutenant General William Shelton, of the 14th Air Force and USSTRATCOM's Joint Functional Component Command for Space (JFCC-Space).

I serve as the Deputy Commander, as you mentioned, of the Joint Functional Component for Space, which we believe is the nation's global single point of contact for coordinating, planning, integrating, controlling and executing the operations part of the Department of Defense forces.

I'm a soldier raised in the operational environment, serving in our Army's Light Aerosol Airborne Divisions, European Air Defense Units, and recently as the Chief of Fires and Effects in the Multinational Corps in Iraq.

I've also had several joint interagency tours with the National Security Agency, NATO, and two tours at U.S. Strategic Command--the latter in positions associated with space, missile defense, and C4I mission areas.

It's from this experience that I can tell you unequivocally that space is clearly a domain--not purely an enabler--that produces the critical capabilities necessary to win our wars, protect our citizens, and empower our global economy.

It's also clear that our operational environment is changing dramatically everyday. We serve with soldiers, sailors, airmen, Marines, civil servants, and a superb industrial support community, the best in the world. They're a dedicated, innovative, joint interagency force, working hard 24 hours a day, seven days a week conducting our nation's space operations. I sincerely stand in awe of their professionalism, commitment and savvy in understanding world affairs and the role that they play, even as junior enlisted members, in preserving our way of life.

I'm humbled to work with them and I find it incredibly valuable to link the experience and knowledge that ground warfighters bring to this problem and the great operational and strategic minds in the professional and national security space profession.

The JFCC Space team provides unity of effort across military, civilian, allied and full spectrum space operations, and we believe yields a tailored responsive global effect to support our national

security mission.

The space domain has fundamentally reshaped our lives in the last 50 years. Today, we depend upon space-based capabilities to conduct commerce, advance our interest and defend our nation. Space impacts nearly every aspect of our lives as individuals and as a nation.

It holds promise for exploration, enhances civil and military operations, including disaster relief efforts and transmits an amazing array of global communications everyday.

Today, space can no longer be seen as either a sanctuary or simply an enabler. We've known this for some time. Space-enabled capabilities impact all warfighting domains, particularly space-based communications and intelligence assets. Space is more than an enabler, as I mentioned. It's also a domain. We must view space activities the same way we regard those in air, land and sea and cyberspace.

As space-based capabilities provide critical support to forces in other domains, space operations must also receive the same support and protection from those very forces that they enable.

China's rapid rise over the recent years as a political and economic power with growing global influence is an important element in today's strategic landscape, one that has significant implications for the region and for the world overall.

However, much uncertainty surrounds China's future course, in particular, in the area of expanding military power and space assets and how that power might be used. China continues to aggressively develop a wide array of space and counterspace capabilities. As they pursue widespread military capability advancement, China views progressive space and counterspace capabilities as essential elements of national prestige and attributes of a national power and a world power.

Their current efforts include establishing a wide array of space and terrestrial-based capabilities to provide reconnaissance, navigation, communications and support to all types of military and civil operations. Recent People's Liberation Army writings also emphasize the necessity for destroying, damaging, and interfering with the enemy's reconnaissance and observation and communications capabilities, suggesting that such systems, as well as satellites and navigation and early warning satellites, could be among the initial targets of any attack to blind and deafen an enemy.

China's space activities/capabilities include ASAT programs and have significant implications for anti-access and area denial in the Taiwan Straits, contingencies and well beyond.

China does not have a discrete space campaign but views space operations as an integral component to everything that they do. To

support their operations, the Chinese continue to build a space architecture consisting of a variety of advanced imagery, reconnaissance and environmental satellites. They currently rely heavily on foreign providers, but are moving aggressively to assure their own capability for the long-term, focused on placing more sophisticated and diverse sets of satellites into orbit, and expecting to replace foreign-produced satellites in its inventory with those they produce themselves by 2010.

China announced traditionally ambitious plans to launch 15 rockets and 17 satellites in 2008. Although such predictions are seldom fulfilled, we need to pay attention to this. Additionally, China announced its intention to launch a third-manned space mission, a Shenzhou 7, in October 2008, on the heels of the Beijing Olympics, underscoring space development as an important symbol of national pride. They intend to conduct a spacewalk at this time.

The majority of the technology used in China's manned space program is derived from Russian equipment and China receives significant help from Russia with specific satellite payloads and applications.

Unfortunately, not all of China's forays into space have been peaceful. In January 2007, China successfully tested a direct ascent anti-satellite weapon, destroying a defunct PRC weather satellite. The unannounced test demonstrated PLA's ability to attack satellites orbiting in low earth orbit and raised worldwide concern. The resulting debris puts at risk the assets of all spacefaring nations, including endangering human space flight.

Our dependence on space and the growing danger posed by numerous hazards requires that we proactively protect our space capabilities. To ensure freedom of action in space for all partners, we need to maintain an acute awareness of all spaceborne objects, hazards and terrestrial threats to space operations to enable and inform deconfliction, improve confidence and responsible actions in space.

Our adversaries understand the asymmetric advantage our space capabilities provide, and also that it constitutes an asymmetric dependence that can be exploited.

Space situational awareness is foundation to space protection, both of which preserve recognition and attribution. Space situational awareness is our number one operational priority. Our understanding of hazards elevates the need to detect, track, characterize, attribute, predict and respond to any threat such that we can observe, orient, decide and act decisively.

The analogy of a 1,000 ship navy built through a coalition of nations can be applied to space, and the ability to leverage and expand space partnerships with our allies holds the potential to dramatically

improve space situational awareness.

Lastly, encouraging military-to-military dialogue through and beyond space situational awareness with all spacefaring nations provides an important opportunity to increase understanding of each other's intentions and to pursue methods to improve multilateral cooperation.

Furthermore, understanding each others' specific perceptions and respective doctrines will ensure our force postures are perceived in their proper context ensuring transparency and building confidence in the protection and sustainability of numerous space capabilities.

China's recent vision endorsed by the 2007 Party's 17th Congress indicated an increasing desire to connect the technical world and the vision of a harmonious working relationship with world superpowers is an important aspect to this problem.

On the subject of space, it behooves all spacefaring nations to work together for the peaceful advancement of this domain that has become absolutely critical for our global way of life. As spacefaring nations, including China, increase their interaction in space, we must continue to see greater engagement opportunities to better understand and create prospects for additional collaboration.

We live in a micro-second world characterized by fast, dynamic, technological change with space operations, information, and potential threats moving all at the speed of light. United States' reliance on space capabilities across our military, civil and economic sectors coupled with the increased and diverse threats to our space assets requires real time playbooks, trained and ready forces operating as a joint and interagency team 24/7 every day.

We appreciate your support and supporting a need for automated change detection tools, enhanced sensors, modeling and simulation tools, and command and control systems to facilitate rapid decision-making and execution.

This is an exciting time to be in the evolution of our global space operations, and I'm truly honored to be serving with such exceptional men and women as they expertly tackle all the challenges that we face today.

Thank you for this opportunity and your continued strong support in all that we do and time to speak to this Commission.

[The statement follows:]

Prepared Statement of Brigadier General Jeffrey C. Horne
Deputy Commander, Joint Functional Component Command for Space, U.S. Strategic Command, Vandenberg Air Force Base, California

Mister Chairman and distinguished Members of the Commission, thank you for the invitation to meet with you today. This commission fills an important role advising Congress on our country's relationship with the People's Republic of China, and I appreciate the opportunity to participate in informing your dialogue, conclusions, and recommendations regarding space issues. It's an honor to be here representing United States Strategic Command (USSTRATCOM). I serve as the Deputy Commander of the Joint Functional Component Command for Space (JFCC-Space), which is the nation's global, single point of contact coordinating, planning, integrating, and operationally controlling military space forces.

I am a soldier raised in the operational environment, serving with our Army's Light, Air Assault, and Airborne Divisions, European Air Defense Units, and recently as the Chief of Fires and Effects in the Multi-National Corps (IRAQ). I also have several Joint and interagency tours at the National Security Agency, the North Atlantic Treaty Organization, and two tours at USSTRATCOM. It is from these experiences that I can tell you unequivocally that Space is clearly a domain that produces the critical capabilities necessary to win our wars, protect our citizens, and empower our global economy. It is also clear that our operating environment is changing dramatically every day.

We serve with incredible Soldiers, Sailors, Airmen, Marines, Civil Service, and a superb industrial support community. They are a dedicated and innovative joint and interagency force, working hard 24 hours a day and 7 days a week conducting our Nation's space operations. I stand in awe of their professionalism, commitment, and savvy in understanding world affairs and the role they play in preserving our way of life. I am humbled to work with them, and I find it incredibly valuable to link experience and knowledge of ground warfighters with the great operational and strategic minds in the professional national security space profession. The JFCC-Space team provides unity of effort across military, civilian, and allied full-spectrum space operations and yields tailored, responsive, global effects in support of national, USSTRATCOM, and geographic command objectives.

The space domain has fundamentally reshaped our lives in the last 50 years. Today, we depend upon space-based capabilities to conduct commerce, advance our interests, and defend our Nation. Space impacts nearly every aspect of our lives—as individuals and as a nation. It holds promise for exploration, enhances civil and military operations, including disaster relief efforts, and transmits an amazing array of global communications. Our daily lives are reliant upon the products that are produced and distributed by our civil and military space systems.

Today, space cannot be seen as either a sanctuary or simply an "enabler." Space-enabled capabilities impact all other war-fighting domains, particularly with space-based intelligence and communications assets. Space is more than an enabler, though—space is also a domain. We must view space activities the same way we regard activities in land, sea, air and cyberspace domains. As space-based capabilities provide critical support to forces in other domains, space operations must also receive support and protection from forces outside the space domain.

China's recent and rapid rise as a political and economic power with growing global influence is an important element in today's strategic landscape, one with significant implications for the region and the world. However, much uncertainty surrounds China's future course, in particular in the area of its expanding military power and how that power might be used.

China continues to aggressively develop a wide array of space and counter-space capabilities. As they pursue widespread military advancement, China views progressive space capabilities as an essential element of national prestige and among the attributes of a world power. Their current efforts include establishing a wide array of space and terrestrial-based capabilities to provide reconnaissance, navigation, and communications support to military operations.

Recent People's Liberation Army writings also emphasize the necessity of "destroying, damaging and interfering with the enemy's reconnaissance/observation and communications satellites," suggesting that such systems, as well as navigation and early warning satellites, could be among initial targets of attack to "blind and deafen the enemy…" China's space capabilities, which include their ASAT programs, hold great implications for potential anti-access/area denial activities in the Taiwan Straits and beyond.

China does not have a discrete space campaign but views space operations as an integral component of all campaigns. To support their operations, the Chinese continue to build a space architecture consisting of a variety of advanced imagery, reconnaissance, and environmental satellites. They currently rely heavily on foreign providers but are moving aggressively to assure their own organic capability for the long term, focused on placing a more sophisticated and diverse set of satellites into orbit and expecting to replace all foreign-produced satellites in its inventory with indigenously produced models by 2010.

China announced traditionally ambitious plans to launch 15 rockets and 17 satellites in 2008, although such predictions are seldom fulfilled. Additionally, China plans a third manned space mission, Shenzhou VII, in October 2008, following the Beijing Olympics and underscoring their space capability as an important symbol of national pride. Most of China's manned space program's technology is derived from Russian equipment, and Russia provides significant assistance for specific satellite payloads and applications.

Unfortunately, not all of China's forays into space have been peaceful. In January 2007, China successfully tested a direct ascent, anti-satellite (ASAT) weapon, destroying a defunct PRC weather satellite. The unannounced test demonstrated the PLA's ability to attack satellites operating in low-Earth orbit and raised worldwide concern. The resulting debris puts at risk the assets of all space-faring nations well into the future, including endangering human space flight.

Our dependence on space and the growing danger posed by numerous hazards requires that we proactively protect our space capabilities. To ensure freedom of action in space for all partners, we need to maintain an acute awareness of all space-borne objects, hazards, and terrestrial threats to space operations, to enable and inform deconfliction, improved confidence, and responsible actions. Potential adversaries understand the asymmetric advantage our space capabilities provide and that it also constitutes dependency that can be exploited. Space Situational Awareness (SSA) is foundational to space protection, both of which preserve recognition and attribution. Requirements for freedom navigation and assured access elevate the need to detect, track, characterize, attribute, predict, and respond to any threat to our space infrastructure. We must continue to foster collaborative data-sharing with our allies to enhance global coverage. The analogy of a one-thousand ship navy built through a coalition of nations can be applied to space, and the ability to leverage and expand space partnerships with our allies holds the potential to dramatically improve Space Situational Awareness.

Lastly, encouraging military to military dialogue through and beyond Space Situational Awareness with all space-faring nations provides an important opportunity to increase understanding of each others' intentions and pursue methods to improve multilateral cooperation. Furthermore, understanding each others' specific perceptions and respective doctrines will ensure our force postures are perceived in their proper context and build confidence in the protection and sustainability of numerous space capabilities.

President Hu Jintao's own ideological formation – "Harmonious World" – emphasizes "diversity" and "equality" in international relations alongside the traditional Chinese foreign policy beliefs of "noninterference" and the "democratization of international relations." This vision was endorsed at the 2007 Party 17th Congress in October. In an increasingly connected, technical world, a vision of working harmoniously among space-faring nations increases its importance.

On the subject of space, it behooves all space faring nations to work together for the peaceful advancement

of this domain that has become absolutely critical to our global way of life. As space-faring nations, including China, increase their interaction in space, we must continue to seek greater engagement opportunities to better understand and create prospects for additional collaboration.

The nature of space operations is rapidly evolving with events in space often occurring at the speed of light. The United States' reliance on space capabilities across our military, civil, and economic sectors, coupled with the increased and diverse threats to our space assets, requires real-time playbooks, trained forces, and automated tools to aide decision making and execution. Modeling and simulation tools, decision aids, and operator alerts form the basis for necessary solution sets. This is an exciting time in the evolution of Joint Space Operations, and I am truly honored to be serving with such exceptional men and women as they expertly tackle the challenges we face every day.

Thank you for this opportunity and for your continued service and strong support as we work to preserve our vital space capabilities and work with all elements of national power to preserve the security of our Nation. I look forward to the opportunity to address your questions.

HEARING COCHAIR BROOKES: Thank you, General. Dr. Tellis.

STATEMENT OF DR. ASHLEY J. TELLIS SENIOR ASSOCIATE, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, WASHINGTON, D.C.

DR. TELLIS: Thank you, Mr. Chairman, for the opportunity to testify before this Commission on the issue of China's space programs. After listening to Brigadier General Horne, I must start by saying that I endorse almost everything that he said in his remarks, and I'm tempted to end my oral presentation on just that note.

However, I think that would be a source of some disappointment to you all. So I will proceed to summarize what is essentially a fairly lengthy paper that I've distributed for your consideration basically by highlighting what I think are key conclusions that I draw in three basic areas:

First, the characteristics of China's space program; second, the characteristics of its military space program, in particular; and finally the impact of these investments on U.S. national security.

Let me start by saying that when one looks at the Chinese space program, it's useful to think of it in summary form as defined by three broad characteristics.

The first is that it is a truly comprehensive program. China is not just another developing country that has capabilities that are discrete and isolated. The Chinese space program essentially is an end-to-end program. It has everything from space science to international cooperation integrated into a whole and designed to serve the purposes of national policy.

The purposes of national policy in this context are essentially the accumulation of Chinese national power and the hope that this accumulation of national power will once again restore China to being a major global power in the international system. So the first element is its comprehensiveness.

The second element is that the program is essentially integrated. It's hard to find within the Chinese space program any clear distinctions between the civilian and the military. In fact, many have characterized the Chinese space program as essentially being a military program which has certain civilian projects undertaken as part of that larger rubric.

The important policy point of consequence of this reality is that any cooperation with China in space must be understood to benefit at some level its military capabilities. So the second element is that the program is integrated.

The third element is that it is really a very focused program. The Chinese have refused to invest in space capabilities that involve a frittering of resources. Rather they have tailored the program to meet very specific developmental and military needs. So don't look to the Chinese space program and hope to see an isomorphic replication of what the U.S. space program looks like. It's a much smaller program, but because China's resources are constrained, it's a program that is tailored very clearly to meeting certain national goals.

To the degree that competition with the U.S. is involved in this program, it's a program that's focused on essentially acquiring technologies from any source at the lowest cost possible and integrating these technologies so acquired to advance Chinese national interests.

Let me say a few words about China's military space capabilities which are the dimension of the space program that assists Chinese military forces. China's military space capabilities are essentially defined by its national military strategy, which is focused on preparing for active defense in the context of local wars which are fought under informationalized conditions.

The essence of this framework is essentially to seek, secure, and maintain information superiority in the context of a conflict.

Because this is the strategic aim of the Chinese military space program, the military space program has three basic dimensions:

China seeks to develop a wide spectrum of capabilities designed to advance its conventional military operations.

The second is that China seeks to develop capabilities that will deny its adversaries access to space.

And third, because there is a clear understanding that space is central to information dominance, China recognizes that a struggle for

space is inevitable and therefore must prepare for it.

Given this fact, most Chinese military space investments today seem to be focused in three broad mission areas:

Developing capabilities for space support. That is essentially being able to launch systems of different kinds into space.

Providing capabilities that enhance force application, that is, the use of military forces, primarily China's conventional military forces.

And third, developing capabilities that allow China to deny the use of space to other more superior adversaries, especially the United States.

To make these aims possible, China has invested capabilities in five basic areas: a very impressive set of systems designed for space launch; a substantial tracking telemetry and control network; a large number of space orbital systems, primarily satellites in different mission areas; a big investment, especially in recent years, with connecting China's space capabilities to its conventional military operators; and finally, a large investment, as the General pointed out, in counterspace technologies, which will only increase over time.

What is the net impact of these military space capabilities? I would urge you to think of it in terms of two dimensions: the space capabilities that are focused on force enhancement primarily allow China today to mount a wide variety of conventional operations with a great deal of confidence, either within its borders or at some distance from its borders.

Over the next decade, the kinds of capabilities that are most certain to come online will allow China to apply force across a much wider spatial domain, to include by the end of the next decade, the Chinese ability to apply power throughout the Western Pacific, at least in certain specific warfighting dimensions.

Where counterspace capabilities are concerned, the basic consequence of counterspace capabilities is that at least in the near term, it allows the Chinese to hold at risk a wide variety of orbital assets, especially those that are in low earth orbit, and as its counterspace capabilities gather steam, it will be able to target orbital systems at much greater altitudes, but even more importantly, to use space as one element in an integrated warfighting strategy that will focus on both command of the electromagnetic and the cyber spectrum.

And it is the synergistic use of space electromagnetic attack and cyber attack that poses, I think, the greatest threat to our warfighters.

Let me end very briefly by giving you my sense of what the strategic implications of these programs are for U.S. national security, and I have five basic conclusions that I'm simply going to telegraph to you.

The first is that Chinese space and counterspace investments

presage an increase in the vulnerability of key U.S. military assets, not only fixed military assets but increasingly mobile military assets, especially power projection assets that have been the currency of U.S. power since the end of the Second World War.

The second point I want to make is that the growth of China's space and counterspace capabilities is part of a change in the balance of power in the Asia Pacific and in the Asian continent more generally.

The third is that the growth of China's space and counterspace capabilities will contribute substantially to raising the costs of American victory in any future conflict with China.

Fourth, they will also have the consequence of expanding the spatial dimensions of the battlefield, both the virtual dimensions and the physical dimensions of the battlefield, in case we are confronted with a conflict in the Pacific region.

And finally, the rise of China's space and counterspace capabilities will pose very specific challenges to American dominance in space, a reality that we have taken for granted for the last 50 years, and so managing China and its space capabilities will be a portion of a much larger problem, which is managing the rise of Chinese power in Asia.

Thank you very much for your hearing.

[The statement follows:][1]

HEARING COCHAIR BROOKES: Thank you.

Mr. Scott, please proceed.

STATEMENT OF MR. WILLIAM B. SCOTT
FORMER BUREAU CHIEF, AVIATION WEEK & SPACE TECHNOLOGY, COAUTHOR: "SPACE WARS: THE FIRST SIX HOURS OF WORLD WAR III"
COLORADO SPRINGS, COLORADO

MR. SCOTT: Thank for you for this opportunity to participate here as a member of this panel.

As General Horne and Dr. Tellis have already outlined, China has some incredible space and cyberspace capabilities. I'll try to add some perspective to their comments.

The People's Republic of China has a rapidly growing, robust space program operated primarily by the Chinese military, and the program's accomplishments are impressive and the plans aggressive. For example:

China has a modern fleet of communication, reconnaissance and

[1] **Click here to read the prepared statement of Dr. Ashley Tellis**

weather satellites and is developing its own space-based navigation constellation similar to the U.S. global positioning system. Most of these spacecraft have both military and civilian applications.

The Chinese Long March family of boosters has posted 100 percent launch success rate over the last ten years. China is developing a new line of rocket engines. Some will burn oxygen/kerosene, and others oxygen/hydrogen fuel. They're scheduled to fly by 2010 and these Long March 5s equipped with these new engines will give China heavy-lift, quote, "rocket capabilities comparable to the U.S. Air Force Evolved Expendable Launch Vehicle, or EELV."

That's according to Craig Covault, Senior Editor for my former employer, Aviation Week.

And very soon China expects to launch a new generation of polar orbit weather satellites. Carrying 11 sensors, the spacecraft will be able to resolve earth surface areas as small as 250 square meters and capture 3-D imagery through clouds.

General Horne noted that China plans to launch its third manned-space mission this October, and one of the three astronauts on that flight will conduct an EVA, extravehicular activity, wearing a new spacesuit developed by Chinese engineers.

The nation plans to eventually build and operate a 20-ton class, manned space station similar to the Russian Mir platform.

China has placed a spacecraft into orbit around the moon and is developing a small rover vehicle to explore the lunar surface around 2015. That may lead to a lunar sample return mission in the 2017 to 2020 time frame, And as we all know, in January 2007, China successfully shot down an aging FY-1C polar orbit weather satellite at an altitude of 537 miles, demonstrating a direct-ascent antisatellite capability. That system has limitations. It's not particularly flexible, but a Chinese ASAT threat definitely exists now, putting many U.S. and allied spacecraft at risk.

As General Kevin Chilton, commander of U.S. STRATCOM, has said, space is no longer a sanctuary. And over the last decade, U.S. satellites and datalinks have been subjected to electronic jamming, laser dazzling, control-network hacking attempts and other forms of interference. China has been responsible for several of these “soft attacks,” demonstrating both a willingness and a capability to target U.S. spacecraft and control networks.

So clearly China has become a world-class spacefaring nation. But that nation's excessive secrecy forces us to ask: what are China's motivations for developing a robust space program? Should we view it as a threat or as an opportunity? On the threat side, China has developed relatively low-cost asymmetric capabilities to disable our

communications, navigation, weather, ISR resources by disabling or destroying key satellites with an ASAT missile. But China may also pose a stealth threat as well. It may already have launched a fleet of micro or nanosatellites and positioned them in close proximity to critical U.S. communications and missile-warning satellites in geostationary orbit, for instance.

Because our space situational awareness resources are limited, we might never find these tiny killersats until they strike.

From a national security perspective, prudence dictates that U.S. military leaders view China's growing space presence and capability as potential threats, then find ways to counteract them.

However, we need to be very careful in exercising counterspace measures. For example, in our second Space Wars book—which is fiction -- and is to be released later this year -- my coauthors and I explore the ramifications of disabling Chinese imaging satellites. We show how temporarily blinding the PLA spacecraft as a means of protecting our own naval forces could unintentionally lead to a shooting war.

And on the opportunity side, U.S. political leaders and citizens would be well served by viewing China's space ambitions from a cultural standpoint. Historically, China has been a major world power and many of its people believe China is now reassuming its rightful place as a leader.

They also have been going to school on what constitutes a global power today: a large powerful military; growing vibrant economy; educated workforce; and a successful space program.

It's important to understand that all these elements are also vital symbols and symbolism is a cornerstone of Chinese culture. In fact, some China experts maintain that an accomplished military-commercial space program is as much a symbol aimed at garnering the support of the Chinese citizens as it is to threaten the U.S. and other spacefaring nations.

Most of all, China wants to be respected. Chinese citizens feel that rather than being congratulated for its rapid development of successful rockets, satellites and lunar probes, for example, China is repeatedly chastised for human rights shortcomings.

In January, Aviation Week and Space Technology chose Qian Xuesen, the father of China's space program, as the magazine's "Person of the Year." That generated a flood of hate mail from outraged readers, but cooler heads saw the choice for what it was: recognition of a man's and a nation's considerable accomplishments in space. Similar forms of recognition and demonstrations of respect might pave the road to space program cooperation and mutual understanding.

To that end, maybe we Americans need to stop sending

conflicting signals. When it comes to China, it seems we haven't decided whether to pursue a policy of containment or one of engagement. Actively promoting cooperative space programs where appropriate might simultaneously foster engagement and what could be termed “deterrence through information.”

For example, if we show China's leaders that shooting missiles at other nation's satellites would create so much orbital debris that nobody could safely launch a spacecraft for decades, perhaps they'd think twice about firing another ASAT.

In short, engagement and dialogue would enable our sending this message loud and clear: conflict in space would be a catastrophe for both the U.S. and China so let's not go there.

Finally, we need to recognize that millions of Chinese citizens admire and greatly respect America. However, U.S. leaders are on the verge of turning those millions of Chinese citizens into rabid America haters.

How? If we boycott the 2008 Olympic Games. If Congress or the administration prevents U.S. athletes from competing in Beijing this summer, again, China experts that I know say it will be viewed as an affront to every man and woman in China, the ultimate humiliation of a proud people.

Their hatred will persist for a generation or more and manifest as a very expensive space race for us and further extension of Chinese military reach. The 2008 Summer Olympic Games are China's coming out party and refusing the nation's invitation will trigger a host of unintended consequences.

So to avoid launching a very costly space race, we must curb ineffective human rights rhetoric and allow U.S. athletes to compete in Beijing. Only then can we hope to find new ways to foster U.S.-China cooperation in space.

Thank you.

[The statement follows:]

Prepared Statement of Mr. William B. Scott
Former Bureau Chief, Aviation Week & Space Technology,
Coauthor: “Space Wars: The First Six Hours of World War III”
Colorado Springs, Colorado

China's Space Capabilities

The People's Republic of China has a rapidly growing, robust space program that serves both civilian and military objectives. Operated by the Chinese military, the program's accomplishments are impressive and its plans aggressive. For example:

China has a modern fleet of communication, reconnaissance and weather satellites, and is developing its own space-based navigation constellation, similar to the U.S. Global Positioning System. Most of these spacecraft have both military and civilian applications.

The Chinese Long March family of boosters has posted a 100% launch-success record over a 10-year period. A Long March costs about half that of Western boosters, such as Europe's Arianespace Ariane V vehicle.

China is developing a new line of rocket engines that will burn oxygen/kerosene and oxygen/hydrogen fuel. Scheduled to fly by 2010, new-engine Long March 5s will give China heavy-lift "rocket capabilities comparable to the U.S. Air Force Evolved Expendable Launch Vehicle (EELV)," according to Craig Covault, Senior Editor for *Aviation Week & Space Technology* magazine (May 5, 2008, p. 29).

This month or next, China expects to launch the first of its new-generation Fengyun-3 polar-orbit weather satellites, which will benefit both People's Liberation Army (PLA) and civilian forecasters. Carrying 11 sensors, the spacecraft will be comparable to mid-1990s versions of U.S. Defense Meteorological Satellite System vehicles. It will be able to resolve Earth-surface areas as small as 250 square meters—which is of particular value for military operations. Further, an onboard microwave sensor will enable creation of three-dimensional images through clouds.

China plans to launch its Shenzou VII this October, marking the nation's third manned space flight. Plans call for one of the three astronauts to conduct an EVA (extravehicular activity), wearing an organically developed spacesuit.

Chinese officials have unveiled plans to perform in-orbit docking of two orbital modules, which will facilitate building and operating a 20-ton-class, manned space station similar to the Russian Mir platform.

China has placed a spacecraft into orbit around the Moon, and is developing a small rover vehicle to explore the lunar surface around 2015. Successful rover operation may lead to a lunar sample-return mission in the 2017-2020 timeframe.

The nation is investing heavily in building a robust space infrastructure to enhance manned space operations. On Apr. 25, China launched the first of two Tianlian relay spacecraft, which will ensure communications with ground controllers throughout most of each Shenzou orbit. The Tianlian system will preclude building a global network of ground stations and is analogous to the U.S. Tracking and Data Relay Satellite network.

Knowing that "intellectual capital"—a competent, well-educated workforce—is the foundation of a vital aerospace sector, China now has about 200,000 engineers and technicians conducting research and development in various disciplines, such as space nuclear power, propulsion, materials, multi-spectral sensors, robotics and myriad other technologies.

In January 2007, China successfully shot down its own aging FY-1C polar-orbit weather satellite at an altitude of 537 miles, demonstrating a direct-ascent antisatellite (ASAT) capability. That system has limitations, and is not particularly flexible, it appears, but a Chinese ASAT threat definitely exists now. That means many U.S. and allied spacecraft in various orbits are at risk of being targeted. Ostensibly, China developed this capability in response to a U.S. ASAT demonstration in the 1980s, when an F-15-launched missile destroyed an aging American satellite in low-Earth orbit.

China's 2007 ASAT test created approximately 2,300 pieces of *observable* orbital debris, triggering strong objections, criticism and denouncements from other spacefaring nations. The test has been described as

"the worst satellite fragmentation event in the 50-year history of spaceflight" (*Aviation Week & Space Technology*, May 12, 2008, p. 36). China's leaders appear to have underestimated the intensity of international reaction, and now regret allowing its R&D sector to conduct the test. Clearly, they also grossly miscalculated the potential impacts of so much debris on all nations' satellites.

The ASAT test shocked many in Congress and the Executive Branch. But it was no surprise to many U.S. military space officials, who have repeatedly sounded warnings about potential threats to U.S. national security, civil and commercial satellites. General Kevin Chilton, commander of U.S. Strategic Command, which is responsible for the nation's milspace operations, noted China has yet to explain its reasons for conducting the test. "It's an important message to the rest of the world," he said. "We oftentimes thought of space as being a sanctuary. Frankly, the U.S. military has not thought that way. But the Chinese [ASAT test] put an exclamation point on that: that it's not a sanctuary; that you do have to worry about people or countries taking you on in this domain, in the event of conflict."

As a reporter for *Aviation Week*, I wrote numerous articles that quoted General Chilton and other leaders of then-U.S. Space Command, its successor, Strategic Command, and the Air Force, Navy and Army space commands, who voiced similar warnings. Those milspace professionals consistently made several key observations: the U.S. is highly dependent on its space infrastructure; that infrastructure is painfully vulnerable, and losing our space assets would be disastrous to U.S. national and economic security. A series of space-related wargames over at least a decade repeatedly underscored the validity of those assessments. However, these articles and generals' testimony seemed to fall on deaf ears in Washington. Consequently, my coauthors and I decided to write a book of fiction, *"Space Wars: The First Six Hours of World War III,"* to tell Americans what *could* happen, if a number of U.S. satellites were systematically disabled via covert attacks.

Attacks in Space

Over the last decade, U.S. satellites and datalinks have been subjected to electronic jamming, laser "dazzling," control-network hacking attempts and other forms of interference. China has been responsible for several of these "soft attacks," demonstrating both a willingness and capability to target U.S. spacecraft and control networks. Consequently, U.S. Strategic Command and its service-level agents are taking prudent measures to protect our satellites, ground stations and uplink/downlink signals. Many of these initiatives are classified, and I'm not cleared for the technical "how" and "what" details. But it's obvious that China's ASAT test served to accelerate these efforts *and* bring badly needed funding to support them. But much more needs to be done to protect U.S. and allied spacecraft.

Since China obviously intends to become a world-class spacefaring nation, it is imperative that U.S. leaders and citizens come to grips with that reality. Should China's growing space capabilities be cause for concern in the West? What are China's motivations for developing such technological strengths, and should we view them as threats or opportunities?

China knows the U.S. has a powerful Navy that can project power via its aircraft carrier groups. Confronting a naval force would be suicidal for China, so the PLA turned its attention to the U.S. Navy's Achilles Heel: a strong dependence on satellites. Thus, China developed a relatively low-cost, asymmetric capability to disable the Navy's space-based communications, navigation, weather and intelligence/surveillance/reconnaissance (ISR) resources by disabling or destroying our satellites. And by demonstrating that capability via an ASAT test, China may force the U.S. to spend prodigious amounts of national treasure to protect our space assets and counter any potential attacks on-orbit.

Another possible asymmetric strategy is China surreptitiously launching a fleet of micro- or nanosatellites and positioning them in close proximity to critical U.S. spacecraft in geostationary orbit. These undetected,

tiny "killersats" could be lurking near some of our huge satellites, waiting for an order to attack and destroy their neighbors. Because our "space situational awareness" or SSA resources are limited, U.S. milspace professionals worry that they may be unaware of such dangerous on-orbit weapons. In fact, "nano-killersats" might already be on-station in GEO, waiting.

Adversary or Partner?

From a national security perspective, prudence dictates that U.S. military leaders view China's growing space presence and capabilities as potential threats, then find ways to mitigate and counteract them as soon as possible. I'm confident that such measures are being taken. But U.S. political leaders and citizens also would be well-served by viewing China's space ambitions, military buildups and phenomenal economic growth from a cultural standpoint.

American and Chinese citizens see the world through vastly different cultural lenses. For example, most Chinese consider their nation's 2,400-year recorded history to be an integral part of a "core belief system." They are justifiably proud of their culture, their society and their myriad accomplishments. Historically, China has been a major world power, a fact its neighbors acknowledge, and central to that power is stability. Confucianism dictates that a nation's stability avoids many ills, such as social unrest and wars that drain resources. America, in China's eyes, is an immature latecomer, in comparison, a nation that somehow rose to greatness despite its seemingly chaotic, "unstable" two-party political system.

Many Chinese believe the period from 1860 to 1949 was an aberration in China's long history, an inward-looking phase that allowed others to become world powers. But the nation's people now believe China is reassuming its rightful place as a major world power, and they have been "going to school" on what constitutes a global power today: a large and powerful military; a growing, vibrant economy; impressive cities with huge buildings; an educated workforce and technological prowess. Finally, China believes that, to be a major world power in the 21st Century, it must be a spacefaring nation, as well.

It's important to understand that all these elements are vital *symbols*, and symbolism is at the foundation of Chinese culture. In fact, some experts on China's culture maintain that a vital, accomplished military-commercial space program is primarily a symbol aimed more at garnering the support of Chinese citizens than to threaten the U.S. and other spacefaring nations. "Space has high visibility and a lot of cache via symbolism in political terms. It 'proves' the effectiveness of [China's] government," says Dr. Noel Miner, Managing Director of International Management Consultants, which facilitates clients' business dealings in China. As Chinese citizens grow suspicious of government effectiveness and corruption, the nation's space program is being leveraged as a powerful symbol of government prowess, Miner and other China experts maintain.

Most of all, China wants to be respected, and, in general, the U.S. has failed to show respect for that nation's economic and technical accomplishments, Chinese citizens feel. Rather than being congratulated for its rapid development of successful rockets, satellites and lunar-probes, for example, China sees U.S. leaders chastising it for human rights shortcomings. Even in this department, China has come far in a relatively brief period. "A hundred and fifty years ago, America didn't have a great human-rights record, either," notes Thomas Menza, a retired U.S. Air Force officer and former Chinese history professor at the Air Force Academy. "China is saying, 'give us credit for what we *have* done!' By harping on human rights, we're creating an enemy, where there doesn't have to be one."

In January, *Aviation Week & Space Technology* named Qian Xuesen the magazine's "Person of the Year," saluting the father of China's space program. This choice generated more than a little hate mail from outraged readers, but cooler heads saw the choice for what it was: respect for a man's—and a nation's—

considerable accomplishments in space. Similar recognition and respectful moves by U.S. political leaders might pave the road to space-program cooperation, rather than creating an adversary.

While it is virtually impossible to decipher China's intentions, America must simultaneously prepare for the possibility of conflict in space, while also making an effort to engage China through cooperative space ventures. The U.S. and Russia successfully separated their military and civilian space programs, then found ways to cooperate on the latter. China should be coaxed into doing the same—although the nation's excessive secrecy regarding space matters is already making engagement a frustrating, lengthy venture. But the potential payoff in reducing mistrust and suspicions is worth the effort.

Cooperative U.S.-China space programs, such as joint deep-space exploration initiatives or having China become an International Space Station partner, would go a long way toward developing mutual respect, understanding and positive relationships among the two nations' space professionals. Such an approach can build on the economic ties our two nations already have forged, which are reducing the chances of terrestrial or in-space conflict.

Deterrence Through Information

Cooperative commercial and civil space programs, guided by a policy of mutually beneficial interaction among U.S. and Chinese space professionals, could lead to what might be termed "deterrence through information." For example, if China's leaders fully understand that shooting dozens of missiles at other nations' satellites would create so much orbital debris that *nobody* could safely launch a spacecraft for years, perhaps they would think twice about firing an ASAT. Further, if they know that America's advanced-technology weapons can disable Chinese satellites at will, *without* creating massive debris fields, and that U.S. satellites can maneuver or otherwise protect themselves, a preemptive ASAT strike miight be deemed inadvisable. In short, the message we should impart is: conflict in space would be a catastrophe for both the U.S. and China, so let's not go there.

Creating a Space Race

Finally, U.S. citizens and their leaders must recognize that roughly 90% of China's approximately one billion citizens admire and greatly respect Americans. Many Chinese want U.S. products, services, music, movies and other elements of Western culture. They have no desire to see our two nations become adversaries. However, U.S. leaders are on the verge of turning a billion Chinese citizens into rabid America-haters, creating a visceral hatred that will persist for a generation or longer. How? By boycotting the 2008 Olympic games. If Congress or the Bush Administration bans U.S. athletes from competing in Beijing this summer, it will be viewed as a slap to the face of every Chinese man and woman—the ultimate humiliation of a proud people. The summer Olympic games are China's coming-out party, and refusing that Asian nation's invitation will trigger a host of unintended consequences. And Americans will suffer greatly for such shortsightedness.

To avoid triggering a very expensive "space race" and giving hardliners justification for building an even larger, more powerful Chinese military force, the Congress and Administration must curb "human rights" rhetoric and allow U.S. athletes to compete in Beijing. Only then can we find new ways to foster U.S.-China cooperation in space.

Panel II: Discussion, Questions and Answers

HEARING COCHAIR BROOKES: Thank you very much. We're

going to move to questions now. I have a number of commissioners who would like to ask questions. If you could all raise a finger to let me know that you want to ask a question during this. If we could just go one question per commissioner in the first round, that would be great.

In my prerogative as cochairman this morning, I'll ask the first question, and I ask this to all of the panelists. The Chinese have made some noise about a new outerspace treaty, perhaps on weaponization of space. Nobody seemed to mention that this morning. And I would be curious of the three panelists as to what you believe the motivation is behind the Chinese desire for a new space treaty?

I'll let you guys decide who is going to respond first.

BRIGADIER GENERAL HORNE: I'll be the first to say it's probably well beyond the realm of my knowledge of their intentions for the space treaty, but I would just offer to pick up on a line from Congresswoman Lofgren: any opportunity to discuss with other nations a way to ensure the peaceful utilization of space would be a positive exchange from my perspective.

I think one of the things we need to encourage from the Chinese certainly is transparency, and that might be a way to get after the discussion and have an open dialogue with them on that particular aspect of their operations.

DR. TELLIS: I think there are two elements to the Chinese interests in what is called PAROS, or the convention to try and outlaw weapons in space.

The first is securing the diplomatic benefits of taking a position that argues for an arms control regime in space. I mean there are very clear benefits to be seen as opposing weaponization of space, trying to construct a peaceful space environment through legal arms control regime, and so there is clearly a diplomatic dimension to the Chinese effort.

But I think there's also a very practical dimension. They seem to have tabled a draft that focuses very much on outlawing weapons in space. And to my mind that is an insufficient instrument because it focuses on just one-half of the threat. It's silent about the threats to systems in space that are not based in space, threats that exist on the ground, and for the foreseeable future, that is, in fact, the most demanding class of threat.

We may reach a point somewhere down the line where we have to deal with the issue of weapons in space, but for the moment, that's not the problem, and because the Chinese instrument--it's a joint Russian-Chinese instrument--focuses so much on weapons in space, one is led to at least ask questions as to why this enormous amount of diplomatic effort is being put into kind of addressing a challenge that's really not

very pressing, and the only answer that my cynical mind can come up with is that it's probably focused on at least making life difficult, for example, for the U.S. ballistic missile defense program because some of the definitions in the treaty instrument really go after components of the U.S. ballistic missile defense program.

And so I see this as again as part of a larger effort to seize the high ground diplomatically but not really solving what I think are the most pressing challenges to space security today.

HEARING COCHAIR BROOKES: Mr. Scott, do you have any thoughts on the issue?

MR. SCOTT: I would just echo the other two speakers. I think if we look at Chinese history, we should proceed very cautiously. We hear them saying one thing, but you have to wonder what they are doing behind the scenes. Even as they laid this proposal on the table, as we know, they conducted an ASAT test.

In short, I think we should listen very carefully to Teddy Roosevelt and follow his advice: speak softly; but carry the big stick.

HEARING COCHAIR BROOKES: Okay. Commissioner Blumenthal.

COMMISSIONER BLUMENTHAL: Yes. Thanks. Thanks a lot to all of you for testifying before us today.

I have a question in terms of how to conceptualize information superiority or supremacy and the space aspects of that type of warfare. Would it be, is it possible for the United States to be able to maintain information or space supremacy/superiority in the way that it does in the air or in the sea?

Is that the right way to think about it? And the corollary to that is, is information warfare, of which you've all described space as a part, an independent form of warfare like some argued air power was strategically, and if so, going back to my original question of can the United States maintain, like it does in the air, superiority over space and the information or electromagnetic spectrum?

That's for all of you.

BRIGADIER GENERAL HORNE: I think you've hit upon one of the great debates, certainly in the Pentagon. The Air Force's view, I believe, is that space supremacy/superiority is definitely something that should be sought, if you will, and I am sure that we would put cyberspace into that same type of a discussion set.

I guess I would offer the notion that what we have to ensure is our freedom of economic, political and military action to defend our interests, and that as long as we can ensure that, then that's what we have to pursue.

But if you proceed in the notion that you just gave us about outer space treaties and what not, the talk of supremacy or superiority

doesn't necessarily lend itself to that type of a discussion. So I think it's a notion of if you regard space as a domain, just like you do air, land and sea, you have to approach it from the standpoint to ensure that your forces, your military, can achieve its actions, and labeling it can be sometimes inflammatory and maybe not particularly helpful.

So I would focus from an operational perspective. As long as we can support our forces, get the information they need to accomplish their objectives, then we're right where we want to be, and labeling it may not be the best approach.

COMMISSIONER BLUMENTHAL: Let me press on that. Air Force doctrine, as everybody knows, is not to engage in operations until we have air superiority. We try to maintain superiority over other domains or the commons. Why is the electromagnetic spectrum different?

Anyone of you can answer that.

DR. TELLIS: I wouldn't make the argument that it's different. I think the real distinction is whether the domain, whether it's space or the electromagnetic spectrum or the cyber environment, whether the domain is a sanctuary or not? If it is a sanctuary, then competition can take place entirely by peaceful means and the outcomes are determined simply by relative differences in technology.

If it's a sanctuary, then the technology that we use to get information is essentially safe, and if I have better technology than you, then I have better information and hopefully I can use that information more effectively.

If, however, you change this boundary condition about whether the domain is a sanctuary, and it becomes contested, then you need more than technology. Then it's not simply a question of whether I have better technology, but whether my technology on balance, that is relative to all your efforts to interfere with my use of the technology, allows me to do what I want, and so I think that is really the critical question.

Now to the degree that we are moving into a political environment where space is going to be less and less of a sanctuary, I think we will have no alternative but to think in terms of information superiority in purely relative terms. That is even as we are collecting information that enhances our ability to conduct military operations, there are others going to be about trying to prevent us from using that information.

And so we have to deal both with the positive uses of the information, which is how do I make my military outputs more efficient, and I have to deal with negating the efforts that the other guy is making to prevent me from accumulating this information in the first place.

If this is the world that we're confronted with, then I think the vision of space will become very soon analogous to the conceptions that we have of air control and sea control and I guess ground control if someone can articulate what that means.

MR. SCOTT: Commissioner, I would just add that perhaps this idea of space supremacy, if we just stick to space for a moment, is a bit of a misnomer. When you use the analogy to air superiority, I think it comes down to a question of when? When we talk about space supremacy, it seems to be received oftentimes as if we establish it now, let's say, and then it's there forever, and that is very inflammatory to many other people.

But if we look at it from the standpoint of having the capability to establish space supremacy in the event of a conflict, not unlike what we do with airpower, then that capability can be viewed as a deterrence.

So people would think twice about trying to, quote, "take the high ground" at any time if they knew that there was a capability in America's hands to not allow that and to ensure that everybody has access to the high ground.

HEARING COCHAIR BROOKES: Commissioner Fiedler.

COMMISSIONER FIEDLER: Thank you. I have two quick questions. Since January 2007, have we gained any greater insight into the Chinese decision-making on the ASAT test? We had some hearings right after that, didn't have a lot of insight. Has anybody gained any insight in the ensuing year and a half or year and three months?

MR. SCOTT: I'll just quote my former employer. They had an article in last week's Aviation Week magazine that said the consensus is moving more and more to the position that Chinese leaders now think that ASAT test was a miscalculation and that they really didn't appreciate the degree of backlash that they would receive. So I think there's a certain level of regret there. At least that's the impression a lot of China-watchers have right now.

COMMISSIONER FIEDLER: Is that recognition that cutting out the Chinese Foreign Ministry was a mistake?

MR. SCOTT: I can't address that.

DR. TELLIS: I think there's a general recognition that the consequences of the test were very problematic to the kind of regime China wants to maintain in space. They were also problematic from the point of view of China's desire to maintain its standing as a responsible player in the international system.

I'm not sure that this equates, however, into a regret about pursuing the program itself, and I think one needs to make a distinction in that regard. The fact that the Chinese have a program I

think tells you something about their intentions. The fact that they chose to test that program in the way that they did certainly in retrospect seems to be something that a wide variety of official Chinese interlocutors seem to regret, but that distinction is very important.

COMMISSIONER FIEDLER: General?

BRIGADIER GENERAL HORNE: Thanks. I think it may be indicative of something that is maybe a little bit more symptomatic, and that is that China is pursuing a broad-based comprehensive transformation of its military, and space is a piece of that.

We've mentioned before that essentially they have a pretty good knowledge management process, that they're able to work with many communities and frankly have put together a pretty impressive program since the late '90s.

That doesn't necessarily mean that they understand the full ramifications across the spectrum of that particular realm. Understanding it technically is not necessarily understanding it across the diplomatic, informational, military, economic aspects of it. And there are cultural challenges worldwide in grasping that, too, and I relate that back to the discussion just a moment ago of I think it was space superiority/space supremacy.

My colleagues mentioned the notion of technology is great, but you have to understand how to apply it across the spectrum, something we call DOTMLPF, a terrible acronym that's tough, but it's about doctrine and organizational and training and a cadre that fully understands how to operate within an environment and facilities. And it goes through the full spectrum of this business.

I think whenever you do something fast, you also leave out some of the details, and I think that's fundamentally probably what the Chinese are experiencing. This is a pretty big, pretty interdependent environment, and maybe their actions had to be sorted through a bit more than they earlier anticipated, and that approach is something they're going to have to take a look at.

COMMISSIONER FIEDLER: Thank you. Just one quick follow-up to what you all said, that there is little distinction between the civilian and military use. That seems to me to create some serious problems for us in defining what is dual use technology in terms of our exports involving space and our cooperation should we engage in it.

Is my concern valid?

DR. TELLIS: I think it's absolutely valid. I mean at a purely technological level itself, it's hard to look at dual-use technology and make clear judgments about where it could be used, but when you look at the Chinese program, which is such an integrated program across the civilian and the military domains, it's even harder, and when you

multiply the problems caused by opacity, the lack of insight into organizational decision-making and chains of command, it becomes even more burdensome.

My own prejudice in this regard is, you know, better to be safe than sorry. If we decide to make dual-use technologies available in any context, we have to make those decisions with malice aforethought where you basically have to do the calculation that says even if this technology so transferred was used to ill purpose, do I have the means to cope with the consequences? And if we can kind of make that calculation, I think that's the only way to deal with this challenge because I don't think you're going to get an essentialist solution to try and figure out what can be transferred and what can't.

HEARING COCHAIR BROOKES: Thank you.

COMMISSIONER FIEDLER: Thank you.

HEARING COCHAIR BROOKES: Commissioner Wessel.

COMMISSIONER WESSEL: Thank you all for your testimony today. I'd like to understand if I can a little better, taking this from concept to reality, I guess, for potentially our troops on the ground. I think, Dr. Tellis, you indicated, to quote you, that "the struggle for space is inevitable," and you went on to make some points about electromagnetic implications.

Space and the electromagnetic spectrum seem to be an integrating factor for our troops on the ground whether you're looking at Predator aircraft aerial views, other integrated information assets that our troops have. Should we be looking at this not just as another sector, not as another service domain, but really as an integrating factor, and aren't the implications of Chinese activities even greater here?

If they were to detonate or use electromagnetic pulse weapons, for example, over a battlefield, wouldn't it create enormous operational problems for all of our activities across the domains?

General, if you could start?

BRIGADIER GENERAL HORNE: Well, I guess I'd start out any time someone detonates a nuclear weapon or generates an electromagnetic pulse anywhere in the world, it's going to create some pretty significant implications for everyone involved.

COMMISSIONER WESSEL: Certainly.

BRIGADIER GENERAL HORNE: And I think that in and of itself may be a deterrent. If they're to conduct that type of activity in space, it's going to create very significant implications for them as well. When you take a look at the growth in their space program, given that they've got about 20 spacecraft in orbit in about 2005, and they're going to grow to somewhere about 90 by 2018, by their projections, it's kind of a double-edged sword. The more they invest

in space, the more they depend on the very capabilities that they're trying to build, the more they emulate what we do, the more vulnerable they are as well.

So as they grow more into this particular environment, they're going to find that they might even be restricting themselves just a bit, not to say a word about, as you just mentioned, about the economic and political impacts of activities in that regard.

So uniquely enough, maybe the more they invest, the more they experience their own restrictions that they would impose upon us.

COMMISSIONER WESSEL: But it is, we should not be, am I correct that we should not simply view it as a separate domain because it does crosscut? Understanding the risks you just said, that unlike air or sea, et cetera, that space now has implications for all of those other domains?

BRIGADIER GENERAL HORNE: Right. You know domain is another one of those emotional words within the military context. I'd take you back to the 1970s when General DePuy laid out something called "AirLand doctrine." It was the beginning of jointness as we know it that wasn't really fully imbibed until frankly Grenada taught us just how limited we were in terms of our interoperability, and that set us forth on a path of jointness from 1983 to 1991 such that when we prosecuted Desert Storm, we had unprecedented levels of understanding of how the domain of air, land and sea interrelate.

So when people talk about space as a domain, I really think that they're talking more of a construct of you need to bring that as a fourth or cyberspace as a fifth entity into that, what was called AirLand doctrine, because the world is much more complex today. We have a compression problem. We're all swimming in the sea of information everyday, and that's going to do nothing but get worse in the days, weeks, and months and years ahead.

So I think the context of a domain is not to isolate it, to say it belongs to a service, but to more relate to the idea that something has to interrelate with those military aspects, and frankly from an interagency perspective across the whole diplomatic, informational, military, and economic perspective, and I think that's where we're at today frankly is we've grown well beyond jointness, and now it's about interagency and international allied cooperation at the same level.

So I believe that you're going to see in the next ten years a move towards interagency domain interrelationships, if you will, of which we're just acknowledging that space is a very key aspect of that. So it's not to isolate it; it's to say that you have to develop it across that DOTMLPF I mentioned earlier and to bring it into the interagency as an integrated component of our national power.

COMMISSIONER WESSEL: Thank you. Either of the other

witnesses?

DR. TELLIS: I wanted to add a different dimension to the issue you raised. I think you put your finger on what to me is really the critical criterion, which is what is the impact of any innovation, especially military space, on warfighting outcomes? I think that should be the question because if you ask it in that way, you begin to see space in this integrated sense, that it's not space per se, but it's space as it affects other inputs, as it were, into the process.

In this context, I think we ought to keep in mind that while the kinetic elements are sexy, you know, the EMP, the ASATs, there are a whole range of technologies out there which are not kinetic. They are more in the soft dimension but could nonetheless have very serious consequences for your warfighting outcomes.

So when one thinks in terms, for example, of say jamming technologies or when one thinks of being able to interdict the link elements between an orbital system and its ground segment, these have real consequences. If you can cut off troops from their communications or from their visibility of what is happening on the other side of the hill at crucial moments in the battle, in the evolution of the battle, you could make a difference to the outcomes even though all the elements of the puzzle are physically intact.

And so I think it's very useful that we use the criteria of the impact on warfighting outcomes as a good metric to judge the significance of innovation, and then we focus not simply on the kinetic systems, or the systems that have kinetic effects, but the softer systems as well, which can be just as consequential.

COMMISSIONER WESSEL: Mr. Scott.

MR. SCOTT: An EMP is a pretty devastating attack on our forces at all levels--strategic, operational and tactical. And after such an attack, you have to assume that those of us who are very heavily dependent on our space assets for sure would be basically blind, deaf and mute in the near term.

So an EMP would have tremendous impacts on the military services as well as the civilian sector. For our warfighting, particularly communications abilities, we do rely on that commercial satellites to carry a lot of noncritical communications traffic, for instance.

So I think that what the Pentagon has to do -- and obviously is doing -- is plan and prepare to, number one, ride it out if you can, protect as much as you can, but if you do suffer a certain amount of degradation, determine how you keep operating?

The old term "graceful degradation" comes to mind because you have to have Plan B, C, and D to keep on operating and do it efficiently. So that requires planning, equipping, training for all of

those eventualities. In our second Space Wars book, we do start it off with an EMP from a high altitude detonation -- and things get messy in a hurry.

COMMISSIONER WESSEL: Thank you.

HEARING COCHAIR BROOKES: Thank you.

Commissioner Shea.

COMMISSIONER SHEA: Thank you all for being here today. Just a quick factual question and then I just have a question for Dr. Tellis. On the factual side, could you tell me how much the PRC spends on space and counterspace activities and whether that amount is included in their annual defense budget?

DR. TELLIS: There are various estimates. The most conservative estimate which Joan Johnson- Freese I think has adduced is about one to $2 billion. The more liberal estimates are close to $5 billion. The problem, however, is that these numbers refer to what is nominally in the space program, and there is much investment in counterspace that does not come under the space program budget.

It comes under other black components of the national budget, and so I think all these numbers have to be taken with a certain degree of caution because they are not indicative of the scale of the program, but having said that, the bottom line is this: the Chinese space program is relatively small compared to the United States. I mean nothing changes that fact irrespective of what the disagreements are. But we need to be cautious about the numbers.

BRIGADIER GENERAL HORNE: I agree with everything that Mr. Tellis just said, and I'll add just a couple things. One, you have to look at how they get their information to build the satellites and the process they're doing. They so far have not had to invest quite the amount of research and development other countries have for the last 40 years to get to where they are.

So I mentioned before the notion of knowledge management. They're pretty good at that--pretty impressive effort so far. Now, innovation, that has yet to be proven, and so innovation usually involves investment to get people all the way through the educational process and then to engender a certain culture to achieve that, again, not necessarily dollars and cents oriented, but you can see how many of their countrymen that are in schools around the world in this particular area, and you'll be pretty impressed. Then also add the notion of labor prices aren't what they are in the United States.

COMMISSIONER SHEA: Right.

BRIGADIER GENERAL HORNE: And they don't have a profit motive. So you add all that together and, you know, one to two, three to five becomes quite a bit less relevant, and then I'd say what you really need to focus on, so what capability--are they really putting on

orbit and, frankly, just as importantly, what are they doing on the ground to be able to leverage that capability to put on orbit, and measure that, and that probably might be the litmus test. The effect that they're actually achieving with that program might be the ultimate measuring stick we might want to use.

COMMISSIONER SHEA: Thank you.

A second question Dr. Tellis, your —response was very helpful. You mentioned there are three elements or characteristics of the Chinese space and counterspace activities: they're comprehensive; it's integrated; and it's focused. So I was hoping you could just flesh out the third element, focused. Focused on what? Focused on a particular military contingency?

DR. TELLIS: I use the term "focused" in multiple ways. It's focused first in the sense of it aims not to replicate the U.S. program. There is a certain economy of logic that the Chinese have used in how they structure the program. They're focused on elements that are important to China, and so I think the prestige elements of the program are things they're happy to benefit from, but I think they think of those as externalities.

They're focused on those elements of the program that aid either national development directly; hence, the great emphasis on, say, communication satellites, on meteorological satellites. They focus on those elements that aid the military program directly. So it's focused in that sense rather than, you know, developing a large sophisticated program for its own sake.

The second element of the question of focus is that they do want their space program to satisfy certain operational military objectives, and so they have, recognizing the fact that they are not as sophisticated, for example, say in microelectronics, and outside the field of developing boosters, their satellite technologies have not been that sophisticated.

So, given these realities and the fact that they're operating in a universe that is still primarily dominated by the U.S., what does focus require of you? Focus requires you to target technologies that you don't have, but which are available elsewhere, and so the Chinese route to innovation, as it were, is really by through joint development of technologies, borrowing, through a lot of activities that are conducted by Western multinational corporations in China, and finally stealing.

And if you listen to public testimony that has been offered in the last year or so, there's been a clear recognition that Chinese espionage activities, primarily in space and dual use, have been at an all-time high. Again, this is an element of focus. So I use the word "focus" in a sort of a omni-directional way because there are many components to it.

COMMISSIONER SHEA: Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Videnieks.

COMMISSIONER VIDENIEKS: Good morning, gentlemen. A quick question. The definition of space sovereignty as viewed by PRC is being almost infinite and limitless, going up to infinity. Our definition relates to the ability to navigate or utilize space. Is there an inherent conflict in whatever scenario we ascribe to the future whether it's conflict or cooperation or managing their space program? Is this something that has to be resolved in the way of a treaty?

MR. SCOTT: I'll take a first shot at that. That may be one realm where we could initially engage the Chinese in a diplomatic way. Perhaps rather than jump all the way to what they're asking for right now -- the no weapons in space, et cetera, et cetera -- we should revisit the way we first dealt with the Soviet Union on space sovereignty. That's part of this deterrence through information I mentioned. If they fully understand that transparency has some real advantages to avoid conflict, then overflights, for instance, in space can have a calming influence.

That's just an initial thought, sir.

COMMISSIONER VIDENIEKS: At this point, though, they have taken a position that they own all space infinitely above their borders.

MR. SCOTT: Then maybe it's time we engaged them and discussed that a bit.

BRIGADIER GENERAL HORNE: Well, I agree with that. I think you're at the leading edge of discussions on how you deal with this new domain as we talked about just a moment earlier. So I think we just deal with it from the standpoint, and this is very early in the process, and engage them, help them see the dichotomy of their very own doctrine where at one point they say blind the enemy, that conflict is inevitable, and then say they don't want to have weapons in space, just doesn't seem to correlate to something that a prudent person would take a look at as a rational approach.

So you engage them and talk to them about that. I think another aspect of it is you mentioned the Cold War. I say display the same level of resolute commitment to being able to maintain your capability throughout the spectrum of conflict, and to do that, of course, we've mentioned space situational awareness, and I'll take yet another opportunity to thank you and Congress for all the great help that we've been given so far and just here recently inside the last year on space situational awareness. That's the first aspect.

Then you have to invest in the ability to make sure that you can conduct graceful degradation, which is a well-used term, and I can tell you given the I deal in it everyday, we do that every single minute of

every single day, working our way through challenges that we see, but prove that you're better at that than anyone else in the world.

Then I'd say you might want to also prove your commitment by your ability to reconstitute. If someone wants to conduct an act that you think is clearly inappropriate, some people would say an act of war, by dedicating some type of a kinetic impact, show that you have a displayed ability to take care of that situation and get assets back on orbit, whether it be air or space, and you can do that in a very quick fashion and be very public about that.

So I think it's a level of, again, using every arrow in your quiver to convince somebody that it's probably not the best investment in the world to go down that approach.

COMMISSIONER VIDENIEKS: To take that, to use that definition, to claim space infinitely above their borders as domain?

BRIGADIER GENERAL HORNE: I think that's a lure that we don't need to bite on.

COMMISSIONER VIDENIEKS: Dr. Tellis.

DR. TELLIS: I agree with the last proposition entirely, that if this is a position that the Chinese have advanced, and there are Chinese military theorists who have talked about it in that way, this is obviously not a position that we can countenance or support.

But to me I think the real challenge is not their conception of sovereignty because I think that is something one can have a conversation about.

The real problem is the actions or the strategies that they seek to employ to defend what they believe is their sovereign right, and it's these actions to the degree that they destroy the notion of space as a sanctuary that become problematic for us.

If we can all agree that it is in our common interest, both Chinese and the U.S. and globally, that we protect space assets because it's not only relevant to military operations but also to larger economic issues, I think we would all come out ahead.

The question is what do you do when you are confronted with a rising power that has very strong political equities that are nonnegotiable and seeks to defend these political equities from what is essentially a position of conventional military weakness? And because China faces itself, finds itself in this situation, it looks for work-arounds that allow it to overcome the limitations of conventional military weakness.

And what it is doing in space is essentially designed to equalize the disadvantages that it currently confronts. And so it's the actions taken in defense of sovereignty rather than some atypical notion of sovereignty itself that I think is at the heart of the problem.

COMMISSIONER VIDENIEKS: Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Mulloy.

COMMISSIONER MULLOY: Thank you, Mr. Chairman. Thank you all for being here with this very helpful testimony.

Mr. Scott, on page four of your testimony, you tell us "historically China has been a major world power," and "many Chinese believe the period from 1860 to 1949 was an aberration in China's long history, an inward-looking phase that allowed others to become world powers."

And you say that China is now "resuming its rightful place as a world power." At least that's their understanding of what they're about.

You further tell us that "America, in China's eyes, is an immature latecomer," "a nation that somehow rose to greatness despite its seemingly chaotic unstable two-party political system." So it seems to me the way you've phrased that, that a two-party democracy isn't sometimes where they aspire to because they look at it as chaotic and unstable.

Mr. Tellis, you make a similar point, on page two of your testimony. I want to put this in a larger context to what we're doing here. You say, "China's space program represents a major investment aimed at enabling Beijing to utilize space in expanding its national power." And you say, and we've heard this before, "the expansion of comprehensive national power has been China's grand strategic objective since at least the reform period initiated in 1978," and that this is critical to China to recover the greatness that it enjoyed for a millennium.

So here have a country that seems to have a game plan, and the game plan is to achieve and restore itself to kind of "numero uno," I think.

Now, is it in the United States' national interest to help China expand its national power? I'll start with you, Mr. Tellis, and then Mr. Scott, and then, General, please feel free to comment. I know you're under constraints when you get into this kind of thing.

DR. TELLIS: I think the short answer to that question is no. The long answer is a little more complicated because if it was a binary choice between helping them increase their national power versus not helping them increase their national power, the answer I think to me at least would be obvious. You don't.

COMMISSIONER MULLOY: Mr. Scott, can you answer? Do you think it's in our interests to help China increase its national power?

MR. SCOTT: I'd have to step sideways on that, sir, and say I don't think we have a choice. They're on track to do that sort of thing.

COMMISSIONER MULLOY: Right.

MR. SCOTT: Then I think we go back to what Dr. Tellis was talking about: how do you work with that and how do you manage as much as you *can* manage and deal with it?

COMMISSIONER MULLOY: Here's my sense. China has a game plan. I don't mind that, and, I'm not hostile to them growing, as long as it's not at our expense. But I get a sense that there's a tremendous transformation going on here, and economic, technological, other power is moving across the Pacific at a pretty rapid pace. They have a game plan. My sense is we have none and that some of our policies are assisting them in achieving their and growing their national power quite rapidly and maybe diminishing our own.

Do you have any comments on that, Mr. Tellis and Mr. Scott? Is that a correct perception?

DR. TELLIS: Let me reframe the problem. This is the point I wanted to make earlier. When I said it's not a binary choice between helping them or not helping them, I think it's not a binary choice because their growth today is inextricably linked with our own.

This is what globalization seems to have done to the international system: that it has made their growth fundamentally dependent on their connectivity with an open economic system, which we value, which we protect, and which we encourage, and so if one tried to prevent China's growth, I think we need to be honest enough to recognize that there would be a penalty that we would pay in terms of our own economic advantage. There is no way to avoid that situation.

So in this environment, what does one do? I mean this is really a question of grand strategy. What kind of a grand strategy do you pursue when you have political competition in an interdependent world?

I don't have a perfectly thought-through end-to-end answer, but I think there are two or three elements that I think we need to pay attention to.

The first thing we need to do is make certain that our crown jewels are not diffused. So I do believe that there are some technological capabilities that the United States has which no matter what our commitment to free trade is ought not to be freely traded away.

The second element is I think we need to pursue some kind of a competitive strategies approach, which is even as China grows through its connectivity with the international system including our own economy, we need to make certain that we can stay ahead of the game and, in fact, increase the distance that we have between ourselves and all the rest coming behind.

And you do this essentially through fundamental changes that you make within the United States, in our innovation system, in our investments in higher education, especially science and mathematics and engineering, things like that.

The third element of the policy that I think you follow is that you try and maintain relations between the U.S. and China and relations with other countries around China's periphery on what I think of as an equilibrium. You don't want relations between the U.S. and China to, in essence, sink or end up in a conflictual situation if we can avoid it.

But a key element to securing that outcome I think is to make certain that the alliance relationships that we currently have with various countries in Asia and the proto-alliances that we are building in different ways with countries who are not formal allies remain in very good repair.

And I think it's some combination of these three elements that allows you to deal with the issue of competition in a world of interdependence.

COMMISSIONER MULLOY: Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Esper.

COMMISSIONER ESPER: Well, thank you, Dr. Tellis. You answered the question I was going to ask, and that I'd still like to ask of the other two, and that is: given the Commission's mandate to make recommendations to Congress on ways to improve our position vis-a-vis China, what policy recommendations would you make?

So I'd like to hear from Mr. Scott and General Horne on that question, and then take it one step further for Dr. Tellis on his last answer. And that is, given the points you made about grand strategy, and they make perfect sense, how then in a globalized world does the United States harmonize its policies and positions vis-a-vis China with its allies and foreign partners? Specifically, how do we work with the EU so that there is a mutual appreciation of this ongoing competition and where that may end up for all the Western countries.

So it's a two-part question, Mr. Scott, but General Horne, if you can answer first, what two or three policy recommendations might you make to Congress to address the issues we've been discussing this morning? And then lastly for Dr. Tellis, the harmonization question.

MR. SCOTT: I would just go back to deciding which it is: engagement or containment? And let whatever the decision is guide our policies.

To bring it down, though, to a very basic level" General Bob Stewart--he was the Army's first astronaut, flew the shuttle and was a spacewalker, too--summed it up very nicely for me. He said it really

comes down to this: there's room on the world stage for any number of large powers, and as long as we help shape a perception that it's not a zero sum game -- either you're number one or we're number one, that sort of thing -- an engagement approach helps us work on that.

But he said the other thing we really have to keep in mind is that China is huge in many, many ways. He said they have three times as many people as we do, so you want to avoid conflict if you can. Always dealing with a smile on your face and firmness as well is probably the best way. Now how you shape that into policies is a challenge, I understand, but first we have to have a guiding principle: is it engagement or is it containment? And I think we really don't have a lot of choice but to work towards engagement where we can.

BRIGADIER GENERAL HORNE: Okay. I'll be the first to say I'm going to speak to you as a soldier. I'm not going to speak to you as a policymaker and I wouldn't be so presumptuous as to say I should make policy recommendations from this point because I'm in an operational environment today.

I think the advice that was just delivered is probably pretty sound from the standpoint that this is a very, very large, potentially very powerful member of the international community. And foremost, you have to take on the aspects of what is a pragmatic prudent approach to dealing with that potential foe.

To put a little bit of a spin on a very well-known comment, keep your friends close and those you're not sure about closer. So I would encourage transparency on the Chinese part. I would encourage us to have a methodology of discussing concerns that we have in a way that's helpful.

And I would always keep in the forefront of our mind that when you have something you depend on, then you protect it as if your life depended on it, and I would ensure that we have the ability to do that. And if for some reason that's threatened, I would ensure that you have ability to respond both in active and passive ways, but certainly be able to reconstitute the capability that you had so that you can continue to prosecute and defend your population.

And lastly, I'd say we're engaged in a war, a war on terror, and I think at the forefront of that is what our country is based on, and that is the freedom to pursue your life the way that you want and to maintain human rights, and I believe that might be the thing that guides us in our relationships with others. As long as we're engaging from that aspect, that we're trying to promote the very values that our volunteer force serves under everyday to protect our country, and we engage to promote that first, and then to ensure our ability to protect those citizens, then that's probably where we need to be.

So if any country is promoting those type of values, we work

with them a certain way. If they're not, we figure out what the advantages are to both, and we deal with it in a prudent fashion. That may be a little bit vague and obtuse, but from someone who's been in harm's way recently, it's really basic.

When you look at our soldiers, sailors, airmen, and Marines and civilians that are serving overseas as contractors and what not, in the end, all they want to read in the newspaper is that their country is doing the right thing by others everyday, and they know that they're out there fighting for that everyday. And when they see that, they'll go on forever.

So just make sure that we come across, as we have with many of our actions, that we're preserving human life and the right to dignity and pursue your rights everyday of your life, and we'll always be on the high ground.

Thank you.

DR. TELLIS: You've asked the most difficult question because I think it challenges us to think about how we can advance those objectives that I just laid out a few minutes ago, and I think there are three broad dimensions I want to flag.

One is we can't do it unilaterally because globalization has put us in this box. I mean in some sense dealing with the Soviet Union was so much easier because we were not interdependent, and so containment was so easy to operationalize. We don't have that option today. So the allies become relevant because globalization gives the Chinese the opportunity that if we acted unilaterally, they could go to others.

And they will go to others to get technology, to get access, to get a whole range of things. So how one manages our relationships with allies becomes critical. I would argue that there are several elements here that we need to keep in mind.

The first is that we need to have a sustained conversation with our allies about what the stakes are. That is we need to reach a common understanding of what the rise of China means not simply for the United States but also for their own security interests. There's often a temptation, primarily among our European allies, to think of the rise of China as something happening out there. You know it's in Pacific Asia; it doesn't affect us directly. You don't have to convince the Japanese and the Russians and the Indians that this is significant, but the Europeans are a different matter.

And the Europeans become critical because they really are a repository of high technologies. This is a center of innovation in the global system of some consequence. So we need to talk to our friends and allies, especially the Europeans, about what the stakes are, and the need to be able to develop at least some minimal common basis for

how one deals with China.

At the very least, to my mind, what this conversation must end up with is an understanding about how we manage technology transfers and arms sales because we don't want to be in a position where as we are attempting to protect our interests with China in the Asia Pacific, other doors get opened to the Chinese with respect to tech transfers and arms sales that completely undermine the efforts that we are making in terms of controls.

This is extremely unfashionable, and people don't want to hear this, but I really think we have to think of some successor to the CoCom arrangement, not aimed necessarily at the Chinese alone, but essentially what are the crown jewels that we collectively want to protect because they're important to us. So I think that is certainly an element.

There's another element of working with allies, and that is we've got to make fundamental political commitments to strengthening our allies themselves as they seek to develop, you know, a good working relationship with China. And we've got to work with our allies to strengthen others who may not be formal allies of the United States but are very important for the outcomes that we want to secure in the Asia Pacific.

And again, we can't do this sitting out of Washington. It has to be done with real engagement with our European and our Asian partners.

The last element I think that completes the whole story is that we've got to continue to engage with China. We've got to continue to emphasize that an open economy, a political evolution that goes in the direction that the General just emphasized, respect for persons ultimately, is something that's going to make the U.S.-China relationship more manageable.

I mean to the degree that China evolves in that direction, many of our concerns about China, they won't disappear, but they will certainly be attenuated. And so I think what you need is, in a sense, this package deal where we consciously renounce unilateralism because it's not going to succeed on this question.

We work with the allies in terms of understanding stakes, developing regimes that help protect our interests, and involve commitments to both strengthening the allies and working with the allies to strengthen others, and then we finally continue to work with the Chinese themselves in the hope that their evolution will move in a direction where they become full partners in a way that we hope they can be.

COMMISSIONER ESPER: Great. Thank you all.

HEARING COCHAIR BROOKES: Thank you, and I want to

thank our witnesses for sharing their thoughts with us today in this very important issue.

The Commission will reconvene at one p.m. for the panel on cyberspace.

[Whereupon, at 12:05 p.m., the hearing recessed, to reconvene at 1:00 p.m., this same day.]

A F T E R N O O N S E S S I O N

PANEL III: PRC CYBER SPACE CAPABILITIES

HEARING COCHAIR BROOKES: Good afternoon. Welcome to U.S.-China Commission and Panel III. I will turn things over to Commissioner Reinsch.

HEARING COCHAIR REINSCH: Thank you. I didn't make a statement this morning. I made one on behalf of Vice Chairman Bartholomew so I did want to open the afternoon with a short comment, if I may.

Welcome back to the audience. I'm pleased to cochair this hearing on the topics that we set forth this morning. In our first panel this afternoon, the Commission is going to explore China's cyber warfare activities. The Commission has found that Chinese military strategists have embraced the use of cyber attacks as a military tactic and part of the Chinese military doctrine.

Such attacks if carried out strategically on a large scale could have catastrophic effects on the target country's critical infrastructure.

The purpose of this panel is to examine what capabilities the Chinese military has developed and what the impact of a potential attack would be on U.S. security and critical infrastructure.

Our last panel of the day will examine China's proliferation practices and nonproliferation commitments. Last year, in its annual report, the Commission concluded that China's nonproliferation record has improved, especially after the establishment of its domestic export control system. However, serious concerns remain about the continued transfer of weapons and technology.

China is a party to numerous nonproliferation agreements which create obligations to prevent the use of weapons of mass destruction and also to prevent the spread of WMD technology, materials and delivery systems.

The United States also is a party to its international agreements on nonproliferation and can play a positive role in encouraging China's compliance. I look to the testimony of our expert witnesses and to the recommendations that they may provide for consideration by the Commission.

Thank you again for participating in the hearing, and we'll return to Commissioner Brookes.

HEARING COCHAIR BROOKES: Thank you.

Our next panel, this panel, will examine China's computer network and cyber warfare capabilities.

Our first speaker is Colonel Gary McAlum. He's the Director of Operations over the Joint Task Force for Network Operations at the

United States Strategic Command.

Colonel McAlum leads a diverse group of over 400 professionals across key functional areas including operations, legal, intelligence, international relations, and strategic planning in support of JTF-GNO's mission to direct the operation and defense of the Department of Defense's global information technology enterprise, the Global Information Grid.

Mr. Timothy Thomas is an analyst at the Foreign Military Studies Office in Fort Leavenworth, Kansas, and a retired U.S. Army Lieutenant Colonel. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low intensity conflict and political-military affairs.

And our third witness today is Dr. James Mulvenon. He is the Director of Advanced Studies and Analysis at Defense Group, Incorporated, in Washington, D.C.

As a specialist on the Chinese military, Dr. Mulvenon's research focuses on Chinese C4ISR, defense research/development/acquisition organizations, and policy, strategic weapons programs, cryptography, and the military and civilian implications of the information revolution in China.

Thank you all for joining us. We'll begin with Colonel McAlum.

STATEMENT OF COL. GARY D. McALUM
DIRECTOR OF OPERATIONS, JOINT TASK FORCE FOR GLOBAL NETWORK OPERATIONS, U.S. STRATEGIC COMMAND
ARLINGTON, VIRGINIA

COLONEL McALUM: Good afternoon, and on behalf of General Croom, the Director of Defense Information Systems Agency, and also dual-hatted as the commander of the Joint Task Force Global Network Operations, appreciate the opportunity to spend a little time with you this afternoon.

I also want to take an opportunity to say I appreciate the opportunity to brief you in a classified session yesterday and as I mentioned yesterday, I just want to remind you that much of what we may talk about today I'm not going to be able to go into in any great level of detail. The things that I will discuss today were derived from open source material or material that has previously been testified to you in open hearings.

Anything that needs to go classified, I'd be willing to take that offline and take it for the record. So I'll do my best to answer your questions today. I look forward to the dialogue, but again I just want

to emphasize much of what we're talking about here today can very quickly go classified.

As a way of background, I just want to clarify for baselining purposes, one slight correction. I'm the Chief of Staff of the JTF-GNO. I was previously the Director of Operations so I have four years of experience in the cyber security business within the DoD and interagency world.

So I do have a perspective that I'm happy to share. It's also important to know that the organization I represent, the JTF-GNO, is a component under U.S. Strategic Command, and General Chilton as the Commander of Strategic Command has the assigned mission within the Department of Defense to direct the operation and defense of DoD networks.

I know you had some questions about organizational constructs. Our Title 10 service components, the Air Force, the Navy, the Army, and so forth, are assigned to under an operational relationship known as “OPCON” or operational control from a cyber security perspective. So something like the Air Force cyber command provides forces to JTF-GNO in executing the security portion of their mission.

Today, I have a couple of slides that I was prepared to brief you. Rather than walking through a prepared testimony, I'd like to use the briefing as an outline.

If you could turn to the first slide, I think it's titled "An Old Chinese Saying," and the quote on there is "If you don't go into the cave of the tiger, how are you going to get its cub." And I think that's a really good backdrop for much of what you're looking at today.

As preparation for this testimony and in attempting to make sure I was value added for this Commission, I looked at a couple of old reports. I looked at your last report to Congress back in November of 2007, and I also looked at your record of hearing from last May as well.

But I went back a little bit further. I went back to a Congressional Research Service report back dated 2001, June 2001, on cyber warfare, and it was a little bit amazing to me that the conclusions that were reached back in 2001, which actually took about two years of work to develop for CRS were much of the same things that you came to conclude in your 2007 report and also reemphasized back in your record of hearings.

So I would tell you up front not a lot has changed. General Cartwright in his testimony to you last year when he was the Strategic Command Commander at that time said in open source hearing, unclassified, China is conducting significant amounts of cyber reconnaissance of many networks to include the Department of Defense. Their purpose is primarily data mining, which we continue to

see today, as well as mapping of networks and identifying potential weak points in a network.

So I would tell you that today we would continue to say that is still the case. We see a significant amount of activity along those lines today. For what purpose? We certainly can't speculate at this point in time.

I would also point out on this slide that it's really important to get the lexicon right. In the open source media and other forums, you hear the term "cyber attack" used rather liberally, and you won't hear anyone in the Department of Defense use that term in the context of cyber reconnaissance or network intrusions. What we are seeing today are network intrusions.

Some people might classify that as a form of cyber espionage. I would not have a problem with that characterization, but the terms "attack" and "intrusion" are very different and the differences are significant in many cases. So, for example, someone breaking on to an Air Force base with a camera and a backpack is a serious event, very serious, and is going to get the security forces and a lot of leadership's attention.

However, that's much different than someone breaking into an Air Force base with a satchel charge ready to plant it somewhere and blow something up. Those are sort of the nuanced differences that I think the lexicon discussion has to take into account.

The other thing I will tell you is timing. In the world that we live in, from an Internet perspective, the cyber world, the effort that it takes to conduct cyber espionage by any actor whether it's a well-funded nation state or a transnational organization or a joyriding hacker, the time that it takes in some cases to go from collecting data and mining data to being disruptive, either accidentally or on purpose, can be very short so therein lies some of our concerns from a DoD perspective, the insignificant amount of time that it takes to very quickly switch from passive to disruptive, if desired.

Next slide, please. I want to spend a couple of slides talking to you about the Internet in general because for us we see the Internet as a great source of information. It enables many of our Net-centric operations. We depend on it in many ways, but at the same time, the Internet in many ways is the Wild West. It's a launching pad for many bad things that happen against not just Department of Defense networks but also U.S. government and private networks. It's a breeding ground for lots of bad things like malicious software and cybercriminal activity.

If you look at the "Top Ten Network Threats," put out by SANS Institute for 2008, you'll recognize many of the things that have been discussed in open source, in open reporting. Some of these I talked

about in more detail in yesterday's classified session as well, but these are the same things that translate into serious threats against Department of Defense networks.

Many of these techniques and tools and technologies can be enhanced through well-funded efforts, especially a nation state level of effort, among many countries that have those capabilities, and some of these cases would be countries like China as well as others. There are also many transnational organizations, criminal elements out there, that use many of these same techniques as well.

There's a huge profit in the cyber crime world, it's a booming economy. They're making money because they're able to compromise banking and personal identifiable information and then turn around and sell it in an underground market. So there's an economic aspect that's driving the cyber criminal element in the Internet as well.

Then there's always the nation state concern. And many of these things we see port directly over into Department of Defense networks.

Next slide. Titled "The Internet Wild West." Just a couple of metrics for you. These metrics were gathered by working through interagency as well as working with Department of Homeland Security, and I think the take-away here is that we are seeing a significant increase in the amount of malicious activity that we get by interacting with the Internet.

And there's lots of reasons for that. Symantec's last Internet security threat report that they just put out a couple of months ago said in the last half of 2007, they detected almost a half a million new malicious code elements out there on the Internet. That was a 571 percent increase from a year before. That is absolutely phenomenal. So when you start thinking about technology solutions to cyber security issues, whether they come from a transnational organization or a nation state threat, the present day sets of tools by themselves are not enough to deal with the threat that we're seeing from the Internet today.

So again a foot stomper here. Malicious activity, whether it's software or whether it's actual hacking, is significantly increasing on the Internet, and that again poses a significant risk to not only the Department of Defense networks but also U.S. government and even private industry as well. They're seeing the same thing. So cyber security is big business today and it's also a huge, ongoing challenge.

Next slide. One of our goals in the Department of Defense is to ensure that we can continue to conduct Net-centric operations. We call it mission assurance.

Much of what we do on our unclassified networks depends on the Internet. So at the same time we need to interact with the Internet at large for lots of good reasons, we also want to do some things to

reduce our exposure to that environment out there which as I said before could be characterized as to Wild West, and when I say reduce our exposure, these are the sorts of things on this slide that we want to try to minimize in terms of making their way on to DoD networks, things like root kits, virus/worms, spyware/adware, and the most difficult one that we're all facing, both on the industry side as well as the U.S. government side, are socially engineered e-mail or phishing attacks, very difficult problem today, especially for folks that are able to really do reconnaissance and understand an organization, their TTPs, how they do business. They understand the people in those organizations so that when you or I receive an e-mail that looks like it's coming from our boss, why wouldn't we open it?

And in many cases, that socially-engineered e-mail has malicious software or payload that takes you to a site that allows your computer to be compromised, many times unbeknownst to you.

So there are lots of reasons that we want to control our interaction between the DoD networks as well as with the Internet.

Next slide. This is our foot-stomper for why we want to do that. Our unclassified network, the NIPRNet is a warfighting system. However, today, it wasn't built along those lines. It grew up over time; it evolved over time to be a significant capability that we have to have available during times of war as well as times of peace.

I listed many of the functions that are out there today. We pay our bills online. We do contracting. We order spare parts. We work deployment orders on the NIPRNet.

DLA, Defense Logistics Agency, Defense Finance and Accounting Service, Transportation Command, many, many other organizations depend on applications and services that have to interact with the Internet as well as with private industry in many cases. So we are very concerned about our exposure to the NIPRNet for all those reasons I've talked about, but at the same time you can see that a well-funded nation state among some of those that we have talked about, including China, are certainly able to exploit that same level of access from the Internet to our networks, should they choose So a huge concern.

Next slide. There's a person that I thought would be invited to testify before the Commission at some point, Mr. Kevin Coleman. He's a Senior Fellow at the Technolytics Institute, recently put out an interesting open source report called the China Cyber Warfare Capabilities Estimate.

I just want to quote him a couple times because I think there's a lot of interesting insight to gain from his report. He points out rightfully that cyber attacks are a major menace in the 21st century because of our dependence on the Internet. We've talked about it from

a Department of Defense perspective, but of course look at how industry uses it today, whether it's banking, whether it's commerce, whether it's national security. We are totally dependent on the Internet and the ability to interact across networks.

So it's a huge target. It's a high value target for those that might want to either exploit it for data mining purposes or potentially exploit it from a disruptive perspective. And I think that the really key point that I extracted from his report was from all available information, one could only conclude as he points out, quote, "that China has the intent and technological capabilities necessary to carry out a cyber attack anywhere in the world at any time."

And to follow back up on General Cartwright's testimony last year, he talked about China continues to look for asymmetric advantage and ways to overcome our technological military advantage that we certainly have today. So we see them in doctrine, we see them in action pursuing those capabilities, and I think that Mr. Coleman's report just emphasizes what we have already seen.

Next slide, please. And I extracted a couple of key points out there just for emphasis, and I think we've touched on these already. Cyber espionage efforts. I think it's been well-known and discussed in many forums that China is actively employed in those. I would simply agree with those observations.

“Aims to achieve global electronic dominance by 2050.” I think folks with various degrees of insight might discuss that date in different forums as well. So the date that they come up with is an interesting date. I think we could have a discussion offline on that if you were interested in talking about that.

“Significant weapons and intelligence and infrastructure in place today.” I would also say I don't think that there's any reason to not think that is the case based on the things that we've seen in the open source reporting.

And they also have money. So this is a lot about organizations and nation states having the funding and the resourcing and the wherewithal to pursue the technologies and the capabilities that are already very prevalent on the Internet, but with well-resourced backing and funding and technological know-how, you're able to take those capabilities to a level that is not easily dectected nor countered.

Next slide. Last couple of slides, I just want to talk a little bit about in general, about what the Department of Defense is doing from a cyber security perspective, and I won't get into any details on these.

Our approach in the Department of Defense is based on defense-in-depth. In other words, we do not believe that there is any one thing that you can do to go out and buy cyber security. We believe it spans

the spectrum of technology, tactics, techniques, procedures, policy, and most importantly, it requires a culture change.

In today's Web 2.0 world, people require instantaneous access to information. They demand instant connectivity. That creates a natural tension with the cyber security folks. So as you try to make a more secure environment to conduct military operations and support military operations, adequate security measures needed to be factored in to the equation.

There is some inherent tension in that effort that we're experiencing in the DoD as we try to find the right balance.

Some of the things that we want to do specifically are, for example, we want to improve perimeter security, but if anyone thinks they can build a cyber Maginot Line, that's impossible to do, but there's a lot of things that we allow into the Department of Defense networks today because we're not doing a very good job filtering them out at the perimeter. We have some exciting efforts underway. We talked about those yesterday in a classified session.

Identity management, authentication and access control, are absolutely foundational to any cyber security effort, whether it's in the Department of Defense, U.S. government or private industry. We've made some great progress with using public key infrastructure and the common access card to better control access to our networks. We've seen some great results from that already. We have a long way to go, but identity management is very critical to what we're doing.

We believe deploying better enterprise tools and standardizing in some cases the type of tools that we're deploying and as much as possible, where we can, take the human out of the decision loop, are also going to help us make some progress in this regard.

I talked about a tool yesterday called the host-based security system. That is an end point solution. It's meant to be on every workstation at some point. The idea there is to take a lot of decision-making out of the end user as much as possible, block bad things coming in and not have them have to make a decision whether or not something looks right.

By itself, it's not a perfect solution but coupled with the other defense-in-depth initiatives, it will improve the situation greatly and it shows great promise in improving overall DoD security.

We talked also yesterday about data at rest. You have to be able to secure the information. You cannot build 100 percent secure network and still stay connected to the Internet. So we're going to put more emphasis on securing data. Primarily in the short term, our focus is going to be on data at rest, on mobile and removable media devices such as thumb drives and laptop computers, but eventually we want to put that same level of emphasis on our work station data and data in

transit as much as possible.

And then I would just tell you the foot stomper is culture change to include focus on training, education, awareness. Changing the culture of how our network is used today as well as how it's managed to one that's much more disciplined like a weapon system.

Next slide. I talked a little bit about this yesterday. I want to emphasize the team sport nature of cybersecurity. Within the Department of Defense, we work with a variety of organizations on a day-to-day basis. The intelligence community, Department of Homeland Security, law enforcement, absolutely critical, and a variety of other organizations.

No one including the U.S. government can do this by themselves, and we depend heavily on industry in many cases to understand the nature of threats, not only to our networks but to our critical infrastructure in some cases. That will continue to be very important to anything that you would recommend in the future.

And then the last slide. I would just like to just use an excerpt from the report that you put out last year, which I found very interesting, very insightful and enlightening. Again, I would just say here that I've seen nothing here that has changed.

Your report concluded that China continues to pursue disruptive means and capabilities in the cyber warfare arena. I would just ditto that. And I also agree with one of your ten recommendations which is to treat this as a holistic problem. It's not a DoD problem; it's a national level issue that has not just U.S. government implications, but also has implications for industry and our economic system as well.

That concludes my slides. I am happy to answer questions either now or later. Thank you.

HEARING COCHAIR BROOKES: Thank you very much, Colonel. We'll do questions at the end.

Mr. Thomas.

STATEMENT OF MR. TIMOTHY L. THOMAS
ANALYST, FOREIGN MILITARY STUDIES OFFICE
FORT LEAVENWORTH, KANSAS

MR. THOMAS: Thank you. My name is Tim Thomas. I work at a place called the Foreign Military Studies Office out at Fort Leavenworth, Kansas. Years ago we were known as the Soviet Army Studies Office, SASO, and when the world changed in 1990-91, with the fall of the Soviet Union, we had to change our focus, too, so we focused on emerging threats. One of those was the information warfare factor. That's basically a little bit of background on how I, a Russian specialist, got into the China area.

Everything that we do in our office is unclassified. We are able on occasion, I won't say often, but on occasion, two or three times a year, to have the opportunity to participate in some conferences with the Chinese. That is where the majority of our information comes from. It's usually first-hand information.

So what I offered you in the books that I sent to you earlier are really a result of either us doing book buying over there or discussions with Chinese IW experts.

I think the thing that I would like to focus on in the next few minutes is just the fact that from my own opinion, based on what I've read, the Chinese approach to information warfare and information operations is really quite different than ours, and it has to do with their cultural transformation, their history. For example, they tend to look for stratagem-technology links.

In this country, we tend to focus an awful lot on technology, period. In the past, the Chinese focused on stratagems as part of their historical development. Now, they really seem to be trying to link technology to stratagems. For example, how do the Chinese use packets of electrons as stratagems? The most recent stratagem technology link that I saw open source was in February of this year where one of the people who write often on information topics listed a series of stratagems: crossing the sea under camouflage, and then he said that would be a data driven attack; looting a burning house would be the illegal use of system files; reversing the positions of the host and the guest would be taking over control of the system.

We see this type of link all the time. Now, it's a little bit easier, I think, to talk about packets of electrons if I give you a little bit different type of example. That would be something like “kill with a borrowed sword.”

We might think in this country quite often that, yes, it's easy for Country A to run electrons through Country B to attack Country C, but we probably wouldn't think of it in terms of a stratagem, “kill with a borrowed sword.”

We might not think in terms of something like “to catch something, first let it go.” An example would be establish a honey pot of information, see what someone comes in and takes or leaves, and then catch them at the time of your choosing.

So that is one of the areas that I think is really different about the way they're doing business.

A second area is that if you're looking for some implied recognition of their computer virus development and attack methods, if you look at some of the teachings in their universities, you do see that reflected in the courses that they offer.

In the book that I gave you called Decoding the Virtual Dragon,

on page 154, they list a series of courses that are being taught in one semester, and those courses include information attack and defense tactics, a study of hacker attack methods, computer virus program design and application, network security protocols, and the list goes on and on.

So there is some evidence there that they're really focused on this area of information security and reconnaissance.

One final thing that I'd like to mention, and that is the area of reconnaissance. People have been talking quite often, as you know, about all the attacks now against England, Germany, New Zealand, Australia, South Korea, Japan, Taiwan, and the United States, which seem to have their origin in China.

Reconnaissance is a very important part of the information warfare technology strategy of China. If you go back to an old stratagem that says, “attain victory before the first battle,” that would be exactly what they're trying to do as they recon sites. They're trying to put the pieces before the first battle so that if, in fact, something ever came to a conflict, they would have the ability to go out and exploit those vulnerabilities that they've uncovered.

So those are the opening comments that I wanted to leave with you. If you're really curious about just how deep these guys do think, I would ask you to go to page 245 of the book called Decoding the Virtual Dragon. I put in there the table of contents from a book called 400 Questions of Information Operations, and for each question, the Chinese gave about a paragraph or two answer to each question, and you will see the type of questions they're asking one another and the explanations they're giving.

It's not just about China but about Russia and India and Japan and the United States, as well as information operations in general or cyber operations.

Thank you.

HEARING COCHAIR BROOKES: Thank you, Mr. Thomas.

Dr. Mulvenon.

STATEMENT OF DR. JAMES MULVENON
DIRECTOR, ADVANCED STUDIES AND ANALYSIS
DEFENSE GROUP, INC., WASHINGTON, D.C.

DR. MULVENON: Thank you, Mr. Chairman. As background, I am a Chinese linguist. At the Center for Intelligence Research and Analysis, I run a team of 12 cleared Chinese linguists where we do contract research for the intelligence community.

Those of you familiar with my career know that a lot of my work over the years has been done in this cyber area. I am also the

chairman of the board of an organization that was set up by Dick Clarke when he was at the White House called the Cyber Conflict Studies Association that is seeking to try and build an academic field or discipline in the United States dedicated to cyber conflict studies, much as we did in the '50s and '60s on nuclear warfare.

And finally, part of my bona fides today is that I am also a victim on a regular basis of Chinese cyber warfare. Most of the China specialists in the Washington, D.C. area on a regular basis for the last 18 to 24 months have been receiving in many cases clumsily crafted with bad Chinglish e-mails but with very potent malware attached to them that is designed, in my view, to exploit possibly some of the sensitive but unclassified material that might be on our machines about the daily workings of what we do here in Washington.

Today, I'd like to briefly address four questions. My remarks that I've submitted for the record go into this in much more detail. The four questions are why is China so focused on cyber? What is their objective? How are they doing it? And finally, just some initial words about what we can do about it.

China is focused on cyber, as the previous speakers have alluded to, because of its asymmetric capability. Of course, I think asymmetric is an overused word. I would define all successful warfare as asymmetric warfare in one sense or another. There's nothing uniquely Chinese about it, but what's also attractive to the Chinese about cyber warfare is the very nature of the Internet, the difficulty of what we call the attribution problem, which provides a layer of plausible deniability for cyber attacks, for computer network attack, that we simply didn't have in other strategic realms like nuclear warfare, where we had systems that at least could tell us the origins of certain attacks.

I call this the Tarzana, California problem because in the absence of anything other than log data, it's often extremely difficult to tell whether that attack is actually coming from China or whether it's some punk kid in Tarzana, California who is spoofing off an insecure Chinese server and hacking back into the Department's networks.

That said, there have been a very small number of cases over the years that we've looked at where we've been able to do that, but it was because the Chinese were very clumsy in that sense. It's an important principle to understand. Having looked at over a thousand intrusion forensics of Chinese origin attacks against the DoD systems over the years, they're not going to be attacking us from a dot.mil domain.

Some of the key elements that we've come to rely upon in the past to separate military-oriented attacks from non-military oriented attacks are not relevant. And more troubling than that, at least one

internal Chinese military source that we've looked at over the years talks about how they actually would exploit the jurisdictional problems that we would have in the United States by originating the attack from within CONUS, but knowing that a completely separate law enforcement apparatus would respond to that attack, and in the window between the time when we actually figured out whether it was actually on behalf of a foreign power, that that's precisely the window that they would need to achieve their strategic objective, which I'll talk about in a minute.

Finally, the Chinese military in particular is focused on cyber warfare as a complement to its other capabilities because of its desire to be able to project power, particularly against U.S. military assets in the continental United States and other areas.

What is their objective? I would argue in peacetime, it's primarily a cyber espionage effort, computer network exploit effort, which is complicated, as other members of this Commission know, when you look at China as the world's information communication technology workshop, when you think about the export control regime, our supply chains for all the China origin information technologies, and even Chinese ownership of submarine cable infrastructure in the Pacific and the implications that that has.

But the other focus, particularly in the military literature that we've been collecting, and we have a very large collection of Chinese language internal military writings on this topic, deals with a scenario that frankly I've been describing to various audiences since the late 1990s, and for me it's been a long trip between there and here, but as early as the late 1990s, the Chinese military was describing a scenario, based on their analysis of the fundamental what their view was, the Achilles' heel of the U.S. military, looking at Desert Storm forward, which in their view was the deployment phase, particularly our reliance on civilian communications backbone, our reliance on the NIPRNet, on the unclassified network, and particularly the automated logistics functions that ride on that in support of the time phased force deployment list and other things related to possible military contingency in the Western Pacific involving Taiwan.

Their argument was very much along the lines of what you would find on the PACOM Web site where PACOM talks about the tyranny of distance in the Pacific.

When they layer upon that things about our, you know, in my view, some misperceptions about our casualty aversion, our aversion to putting forces in harm's way without a full force protection package in place, the argument is that by disrupting this unclassified network, by disrupting that, and taking advantage of our standard operating procedures would be to take the network down and go through it with a

nit comb looking for Trojans and back doors and everything else, that they could actually create a window in which they would delay our deployment to a Taiwan scenario sufficient that when combined with kinetic attacks against Taiwan, psychological operations, special forces, cyber attacks, that the Taiwans would look to the east for the cavalry, would see that the cavalry wasn't going to be there in time, and they would capitulate to Beijing.

So it's not a defeat, it's not a destruct mission. What's very striking in the military literature is the argument that they make that, in fact, the worst thing they could do would be to carry out large-scale computer network attacks against U.S. critical infrastructure, financial networks, data and power grids.

They want to do a very precise attack against unclassified military networks. Their argument is if they attack those other networks, they will, in fact, undermine their strategic objective by, quote, "stiffening the backbone of the American people and arousing their natural tendency for vengeance," which is always one of my favorite Chinese quotes.

Now how do they do this or how do they plan to do this? I think that the evidence is pretty clear that the state versus non-state actor distinction is a false one, that in the Chinese case as in the Russia and Estonia case from last year, we're confronted with a hybrid threat which makes the attribution problem even more difficult, particularly the patriotic hacker phenomenon in China which we've looked at very closely.

I've always argued that I do not believe the patriotic hackers are dedicated government agents, but I do believe that they are treated as useful idiots by the Chinese regime, and that the Chinese regime has figured out a rough method, using the propaganda apparatus, to shape the behavior of these patriotic hacker groups, many of whom are getting older and going from black hat to gray hat to white hat, and they want wives and jobs and houses, and the only way to get certified as an information security professional in China is to be certified by the ministries of public and state security.

And so there is a trend line over time that brings groups like X Focus and NSFOCUS and other of those better patriotic hacker groups closer to the government, but I would argue that they also present a very interesting command and control problem for Beijing that Beijing has struggles about and writes about.

In other words, if they're trying to carry out some kind of carefully calibrated coercion campaign against Taiwan, the noise that the patriotic hackers have created in the crises we've had over the last ten years in some cases could obfuscate some of the signaling from Beijing.

So they argue that the patriotic hackers are not always working on the same purpose as the military and, in fact, have to be, their behavior has to be shaped because it could, in fact, undermine the military objective.

In terms of capabilities, therefore, I would suggest not that we reify the Russians in elegant coding and all their mathematicians and everything else, but in fact we apply a simple means/ends test. That we take what the Chinese write about what they want to do in the military realm, what they need to do it, and what we would find is we can lower the bar significantly on our capabilities assessment because often what they describe simply requires access to the Internet, some distributed denial of service tools that can be downloaded off thousands of sites anywhere around the world, and do not necessarily require high levels of sophistication.

On the espionage and exploit side, however, it does require, I think, a higher degree of sophistication, and so there are some interesting cross-cutting analysis that we've done looking at those two things.

Finally, what can we do about it? I agree 110 percent with the colonel, perimeter defense is never enough. Defense-in-depth is important, is absolutely critical. Frankly, changing the mind-set that we're going to be operating in a world in which the potential adversary is always going to be inside the fence line, rather than one in which we can fantasize about them being outside the fence line.

Now, the more controversial aspect of it, and that we can't go into today, is that in some cases, the best defense is a good offense, and that the closer you are to the point of origin of the attack, the easier it is to potentially mitigate some of the attribution problem that led you down this road in the first place.

But just to close, I remember being asked once by a PACOM commander in 1997 if we have this attribution problem, but I see the Chinese engaging in missile exercises and saber rattling and they're trying to intimidate the Taiwans and everything else is going on, and at the same time I see a distributed denial of service attack against PACOM's NIPRNet networks that looks like it's designed to disable my ability to do logistics deployment, does the attribution problem really matter all that much?

And my answer was "No, Admiral, two plus two equals 47; Katy, bar the door." So there's a point at which I think the attribution problem can cease to be relevant in a wartime environment, but in a peacetime environment, it's absolutely critical, particularly given the fact that China has so many insecure networks and is so well-known now for being engaged in activities involving U.S. servers, that we now have to ponder the possibility that other adversaries, in fact, are

routing their traffic through China, through insecure servers in China, and further complicating the attribution of those kinds of activities.

But I look forward to your questions. Thank you very much.

Prepared Statement of Dr. James Mulvenon
Director, Advanced Studies and Analysis
Defense Group, Inc., Washington, D.C.

Thank you, Mr. Chairman and the other members of the U.S.-China Economic and Security Review Commission for the opportunity to take part in the hearings you are holding today on the topic of "China's Proliferation Practices and the Development of its Cyber and Space Warfare Capabilities." My remarks will focus on Chinese cyber capabilities.

Before looking at Chinese thinking and capabilities on computer network operations, however, it is important to contextualize Beijing's interest in the subject within the larger strategic context. In the minds of the Chinese leadership, the available evidence suggests that the most important political-military challenge and the most likely flashpoint for Sino-US conflict is Taiwan. In seeking to reunify the island with the mainland, however, it is important to note that the PRC has a political strategy with a military component, not a military strategy with a political component. The PRC would prefer to win without fighting, since Beijing's worst case outcome is a failed operation that would result in *de facto* independence for Taiwan. Also, the leadership realizes that attacking Taiwan with kinetic weapons will result in significant international opprobrium and make the native population ungovernable. These assumptions explain why China until recently maintained a "wait and see" attitude towards Taiwan, even though the island elected a President from a party committed previously to independence. From 2000 until late 2003, China eschewed saber-rattling in favor of economic enticement and "united front" cooperation with the Pan-Blue opposition, both of which were believed to be working successfully. In November 2003, in response to perceived provocations by Taiwan President Chen Shui-bian, Beijing once again revived the threat of military force to deter what it saw as further slippage towards independence, dramatically increasing tensions in the U.S., China, Taiwan triangle.

Should the situation deteriorate into direct military conflict, the PLA since 1992 has been hard at work bolstering the hedging options of the leadership, developing advanced campaign doctrines, testing the concepts in increasingly complex training and exercises, and integrating new indigenous and imported weapons systems. At the strategic level, the writings of Chinese military authors suggest that there are two main centers of gravity in a Taiwan scenario. The first of these is the will of the Taiwanese people, which they hope to undermine through exercises, missile attacks, SOF operations, and other operations that have a psyop focus. Based on intelligence from the 1995-1996 exercises, as well as public opinion polling in Taiwan, China appears to have concluded that the Taiwanese people do not have the stomach for conflict and will therefore sue for peace after suffering only a small amount of pain. The second center of gravity is the will and capability of the United States to intervene decisively in a cross-strait conflict. In a strategic sense, China has traditionally believed that its ICBM inventory, which is capable of striking CONUS, will serve as a deterrent to US intervention or at least a brake on escalation. Closer to Taiwan, the PLA has been engaged in an active program of equipment modernization, purchasing niche anti-access, area-denial capabilities such as long-range cruise missiles and submarines to shape the operational calculus of the American carrier battle group commander on station. At the same time, a key lesson learned from analyzing U.S. military operations since DESERT STORM was the vulnerability of the logistics and deployment system.

CENTER OF GRAVITY NUMBER ONE: THE WILL OF THE PEOPLE ON TAIWAN

Chinese strategies to manipulate the national psychology of the populace and leadership on Taiwan involve the full spectrum of information operations, including psychological operations, special operations, computer network operations, and intelligence operations. To this end, Beijing can employ all of the social, economic, political and military tools of Chinese national power, as well as enlist the assistance of private sector players and sympathetic co-conspirators on Taiwan. The goal of these efforts is to shake the widely perceived psychological fragility of the populace, causing the government to prematurely capitulate to political negotiations with the mainland. In a sense, China seeks to use the immaturity of Taiwanese democracy against itself.

Analysis of both Beijing's strategies in this arena as well as Taipei's ability to resist such methods confirms Taiwan's high level vulnerability to Chinese soft coercion, and raises major questions about the island's viability in the opening phase of a PRC coercion campaign, their credibility as an source of intelligence information on the mainland and a keeper of U.S. secrets, and their expected ability to interoperate successfully with U.S. forces in a crisis.

Taiwan's vulnerabilities in the critical infrastructure protection arena can be divided into two categories: informational and physical. On the information side, Taiwan is a highly information-dependent society with a relatively low level of information or computer security. Significant disruptions in information systems could have major negative effects on the island, particularly in the economic and financial realms, and increase fear and panic among the population. Past Chinese uses of regional media to send psychological operations messages have also enjoyed success in affecting popular morale and public opinion. For example, an Internet rumor in 1999 that a Chinese Su-27 had shot down a Taiwan aircraft caused the Taipei stock market to drop more than two percent in less than four hours.

On the physical side of the equation, Taiwan's current capability and readiness level is much lower than one might expect for a state under such a direct level of threat, especially when compared with other "national security states" like Israel or South Korea. Critical infrastructure protection has been a low priority for the government, and Taiwan is acutely vulnerable to Spetnaz-like or fifth column operations, aided significantly by ethnic and linguistic homogeneity and significant cross-border flows, which facilitate entry and access to potential targets. In terms of civilian infrastructure, Taiwan's telecommunications, electric power, and transportation infrastructure are all highly susceptible to sabotage. These weaknesses have been indirectly exposed by periodic natural disasters, such as the September 1999 earthquake and the September 2001 typhoon, when the communications infrastructure effectively collapsed. Taiwan's ports, including Su'ao, Jeelung, and Gaoxiong (the third highest volume container port in the world), are attractive targets. Port charts and ship movements are available on the Internet, and Gaoxiong in particular has two narrow mouths that could easily be blocked with scuttled vessels. Taiwan's highways are a vulnerable bottleneck, particularly given the large number of undefended mountain tunnels and bridges that could be destroyed by SOF units. Finally, the power grid is known to be fragile, marked by numerous single-point failure nodes, and no cross-hatching of sub-grids to form redundancy. The loss of a single tower in the central mountainous region, thanks to a landslide, knocked out ninety percent of the grid a couple of years ago, and delays in construction of a fourth nuclear plan have constrained capacity.

Special operations forces and fifth column are also a major threat for disruption of military command and control and decapitation of the national command authority, as well as providing reconnaissance for initial missile and air strikes and battle damage assessments (BDA) for follow-on strikes. Entry into the country for special operations forces is not a substantial obstacle, thanks to ethnic and linguistic homogeneity and the dramatic increases in cross-strait people flows. Between 1988 and October 2002, for example, more than 828,000 mainlanders visited the island. Moreover, these special forces could also facilitate control of key civilian and military airfields and ports that could be used as points of entry for invading forces. The

lack of operational security at key facilities is particularly inexplicable and appalling. Visits to national political and military command centers reveal them to relatively unguarded with poor information security practices, including the use of personal cell phones in supposedly secure areas. The Presidential Palace in downtown Taipei, home to the President and his key staff, has no fenceline and no security checkpoints. Building information, including the location of the President's office, is openly available on the Internet. Given the poor performance of President Chen's personal security detail during the recent assassination attempt on his life, the possibility of elimination of the top leadership through direct action cannot be discounted.

Finally, there is substantial open source evidence to suggest that China is winning the intelligence war across the strait, raising serious doubts about the purity of Taiwanese intelligence proffered to the U.S., the safety of advanced military technologies transferred to the island, and the ability of official Taiwan interlocutors to safeguard shared U.S. secrets about intelligence collection or joint warplanning. In the last five years, a steady series of leaked stories have appeared in the Taiwan and other regional media, describing either the rounding up of Taiwanese agent networks on the mainland or the unmasking of high-ranking Taiwanese agents in the military, with similar successes a rarity on the Taiwan side, despite significant political incentive to publicize such discoveries. Reported examples since only early 2003 include the arrest of the president of the PLA Air Force Command Academy, Major-Genera Liu Guangzhi, his former deputy, Major-General Li Suolin, and ten of their subordinates; the arrest of 24 Taiwanese and 19 mainlanders in late 2003; the arrest of Chang Hsu-min, 27, and his 24-year-old girlfriend Yu Shi-ping; the arrest of Xu Jianchi; the arrest of Ma Peiming in February 2003; and the arrest and conviction to life imprisonment of Petty officer first class Liu Yueh-lung for passing naval communications codes to the PRC. Farther back, high-profile intelligence losses include the discovery, arrest and execution of General Logistics Department Lieutenant-General Liu Liankun and Senior Colonel Shao Zhengzhong as a result of Taiwanese government intelligence disclosures about the fact that warheads on Chinese missiles fired near the island in 1996 were unarmed, the arrest and sentencing of Hainan Province deputy head Lin Kecheng and nine others in 1999 for providing economic, political and other kinds of intelligence to the Taiwan Military Intelligence Bureau, and the arrest and imprisonment of a local official in Nanchong, Sichuan named Wang Ping for allegedly also working for the MIB. In addition, retired senior Taiwan intelligence officials, including National Security Bureau personnel chief Pan Hsi-hsien and at least one former J-2, continue to travel to and often residence in China despite Taiwan regulations barring such movement for three years after retirement. At the same time, Taiwan and international media is regularly filled with leaks about sensitive U.S.-Taiwan military interactions or weapons transfers, sourced to either legislators or standing Taiwan government officials. Examples include disclosures about possible deployment of an Integrated Underwater Surveillance System (IUSS) north and south of the island to detect Chinese submarines, the provision of early warning data on Chinese missile attack from the Defense Support Program (DSP) satellite constellation, and the alleged SIGINT cooperation between the National Security Agency and Taiwan on Yangming Mountain. All of these possible compromises raise serious concerns about future technology or information sharing with Taiwan.

CENTER OF GRAVITY NUMBER TWO: U.S. MILITARY INTERVENTION

Strategies for Attacking U.S. Logistics

When Chinese strategists contemplate how to affect U.S. deployments, they confront the limitations of their current conventional force, which does not have range sufficient to interdict U.S. facilities or assets beyond the Japanese home islands. Nuclear options, while theoretically available, are nonetheless far too escalatory to be used so early in the conflict. Theater missile systems, which are possibly moving to a mixture of conventional and nuclear warheads, could be used against Japan or Guam, but uncertainties about the nature of a given warhead would likely generate responses similar to the nuclear scenario. According to the predictable cadre of "true believers," both of the centers of gravity identified above can

be attacked using computer network operations. In the first case, the Chinese IO community believes that CNO will play a useful psychological role in undermining the will of the Taiwanese people by attacking infrastructure and economic vitality. In the second case, the Chinese IO community envisions computer network effectively deterring or delaying US intervention and cause pain sufficient to compel Taipei to capitulate before the US arrives. The remainder of this section outlines how these IO theorists propose operationalizing such a strategy.

General IO and Computer Network Attack Analysis

Before examining this scenario in detail, it is first necessary to provide some background regarding Chinese views of information operations in general, and computer network operations in particular. At the strategic level, contemporary writers view IO and CNO as a useful supplements to conventional warfighting capability, and powerful asymmetric options for "overcoming the superior with the inferior." According to one PRC author, "computer network attack is one of the most effective means for a weak military to fight a strong one." Yet another important theme in Chinese writings on CNO is the use of computer network attack as the spearpoint of deterrence. Emphasizing the potential role of CNA in this type of signaling, a PRC strategist writes that "We must send a message to the enemy through computer network attack, forcing the enemy to give up without fighting." Computer network attack is particularly attractive to the PLA, since it has a longer range than their conventional power projection assets. This allows the PLA to "reach out and touch" the U.S., even in the continental United States. "Thanks to computers," one strategist writes, " long-distance surveillance and accurate, powerful and long-distance attacks are now available to our military." Yet computer network attack is also believed to enjoy a high degree of "plausible deniability," rendering it a possible tool of strategic denial and deception. As one source notes, "An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from an enemy."

It is important to note that Chinese CNA doctrine focuses on disruption and paralysis, not destruction. Philosophically and historically, the evolving doctrine draws inspiration from Mao Zedong' theory of "protracted war," in which he argued that "we must as far as possible seal up the enemies' eyes and ears, and make them become blind and deaf, and we must as far as possible confuse the minds of their commanders and turn them into madmen, using this to achieve our own victory." In the modem age, one authoritative source states: "computer warfare targets computers - the core of weapons systems and C4I systems - in order to paralyze the enemy." The goal of this paralyzing attack is to inflict a "mortal blow" [zhiming daji 致命打], though this does not necessarily refer to defeat. Instead, Chinese analysts often speak of using these attacks to deter the enemy, or to raise the costs of conflict to an unacceptable level. Specifically, computer network attacks on non-military targets are designed to "...shake war resoluteness, destroy war potential and win the upper hand in war," thus undermining the political will of the population for participation in military conflict.

At an operational level, the emerging Chinese IO strategy has five key features. First, Chinese authors emphasize defense as the top priority, and chastise American theorists for their "fetish of the offensive." In interviews, analysts assert their belief that the US is already carrying out extensive computer network exploit activities against Chinese servers. As a result, CND must be the highest priority in peacetime, and only after that problem is solved can they consider "tactical counteroffensives." Second, IW is viewed as an unconventional warfare weapon to be used in the opening phase of the conflict, not a battlefield force multiplier that can be employed during every phase of the war. PLA analysts believe that a bolt from the blue at the beginning is necessary, because the enemy may simply unplug the network, denying them access to the target set, or patch the relevant vulnerabilities, thus obviating all prior intelligence preparation of the battlefield. Third, IW is seen as a tool to permit China to fight and win an information campaign, precluding the need for conventional military action. Fourth, China's enemies, in particular the United

States, are seen as "information dependent," while China is not. This latter point is an interesting misperception, given that the current Chinese C4I modernization is paradoxically making them more vulnerable to US methods.

Perhaps most significant, computer network attack is characterized as a preemption weapon to be used under the rubric of the rising Chinese strategy of *xianfa zhiren*, or "gaining mastery before the enemy has struck." Preemption [xianfa zhiren 先　制人] is a core concept of emerging Chinese military doctrine. One author recommends that an effective strategy by which the weaker party can overcome its more powerful enemy is "to take advantage of serious gaps in the deployment of forces by the enemy with a high tech edge by launching a preemptive strike during the early phase of the war or in the preparations leading to the offensive." Confirming earlier analysis of Chinese views of U.S. operational vulnerabilities in the deployment phase, the reason for striking is that the "enemy is most vulnerable during the early phase of the war." In terms of specific targets, the author asserts that "we should zero in on the hubs and other crucial links in the system that moves enemy troops as well as the war-making machine, such as harbors, airports, means of transportation, battlefield installations, and the communications, command and control and information systems." If these targets are not attacked or the attack fails, the "high-tech equipped enemy" will amass troops and deploy hardware swiftly to the war zone, where it will carry out "large-scale airstrikes in an attempt to weaken...China's combat capability." More recent and authoritative sources expand on this view. "In order to control information power," one source states, "there must also be preemption.. .information offensives mainly rely on distant battle and stealth in order to be effective, and are best used as a surprise...Therefore, it is clear that whoever strikes first has the advantage." "The best defense is offense," according to the authors of *Information Operations.* "We must launch preemptive attacks to disrupt and destroy enemy computer systems."

Specific Targeting Analysis of Network Attacks Against Logistics

There are two macro-level targets for Chinese computer network operations: military network information and military information stored on networks. Computer network attack seeks to use the former to degrade the latter. Like US doctrine, Chinese CNA targeting therefore focuses specifically on "enemy C2 centers," especially "enemy information systems." Of these information systems, PLA writings and interviews suggest that logistics computer systems are a top military target. According to one PLA source, "we must zero in on the...crucial links in the system that move enemy troops... such as information systems." Another source writes, “we must attack system information accuracy, timeliness of information, and reliability of information.” In addition to logistics computer systems, another key military target for Chinese CNA is military reliance on civilian communications systems.

These concepts, combined with the earlier analysis of the PLA view that the main US weakness is the deployment phase, lead PLA IO theorists to conclude that US dependence on computer systems, particularly logistics systems, is a weak link that could potentially be exploited through computer network attack. Specifically, Chinese authors highlight DoD’s need to use the civilian backbone and unclassified computer networks (i.e., NIPRNET) as an "Achilles Heel." There is also recognition of the fact that operations in the Pacific are especially reliant on precisely coordinated transportation, communications, and logistics networks, given the “tyranny of distance” in the theater. PLA strategists believe that a disruptive computer network attack against these systems or affiliated civilian systems could potentially delay or degrade U.S. force deployment to the region while allowing the PRC to maintain a degree of plausible deniability.

The Chinese are right to highlight the NIPRNET as an attractive and accessible target, unlike its classified counterparts. It is attractive because it contains and transmits critical deployment information in the all-important TPFDL (time-phased force deployment list), which is valuable for both intelligence-gathering about US military operations but also a lucrative target for disruptive attacks. In terms of accessibility, it is relatively easy to gather data about the NIRPNET from open sources, at least before 9/11. Moreover, the very nature of system is the source of its vulnerabilities, since it has to be unclassified and connected to the

greater global network, albeit through protected gateways. To migrate all of the NIPRNET to a secure, air-gapped network would likely tax the resources and bandwidth of DOD's military networks.
DoD’s classified networks, on the other hand, are an attractive but less accessible target for the Chinese. On the one hand, these networks would be an intelligence gold mine, and is likely a priority computer network exploit target. On the other hand, they are a less attractive computer network attack target, however, thanks to the difficulty of penetrating its defenses. Any overall Chinese military strategy predicated on a high degree of success in penetrating these networks during crisis or war is a high-risk venture, and increases the chances of failure of the overall effort to an unacceptable level. Moreover, internal PRC writings on information warfare show no confidence in the PRC's ability to get inside network-centric warfare aboard deployed ships or other self-contained operational units. Instead, the literature is focused on preventing the units from deploying in the first place, and thereafter breaking the C4I linkages between the ships and their headquarters.

Chinese CNE or CNA operations against logistics networks could have a detrimental impact on US logistics support to operations. PRC computer network exploit activities directed against US military logistics networks could reveal force deployment information, such as the names of ships deployed, readiness status of various units, timing and destination of deployments, and rendezvous schedules. This is especially important for the Chinese in times of crisis, since the PRC in peacetime utilizes US military web sites and newspapers as a principal source for deployment information. An article in October 2001 in *People's Daily*, for example, explicitly cited US Navy web sites for information about the origins, destination and purpose of two carrier battle groups exercising in the South China Sea. Since the quantity and quality of deployment information on open websites has been dramatically reduced after 9/11, the intelligence benefits (necessity?) of exploiting the NIPRNET have become even more paramount. Computer network attack could also delay re-supply to the theater by misdirecting stores, fuel, and munitions, corrupting or deleting inventory files, and thereby hindering mission capability.

The advantages to this strategy are numerous: (1) it is available to the PLA in the near-term; (2) it does not require the PLA to be able to attack/invade Taiwan with air/sea assets; (3) it has a reasonable level of deniability, provided that the attack is sophisticated enough to prevent tracing; (4) it exploits perceived US casualty aversion, over-attention to force protection, the tyranny of distance in the Pacific, and US dependence on information systems; and (5) it could achieve the desired operational and psychological effects: deterrence of US response or degrading of deployments.

CONCLUSIONS: IS THE SCENARIO REALISTIC?

Chinese IO theorists assert that computer networks attacks against unclassified computer systems or affiliated civilian systems, combined with a coordinated campaign of short-range ballistic missile attacks, "fifth column," and IW attacks against Taiwanese critical infrastructure, could quickly force Taiwan to capitulate to Beijing. This strategy exploits serious vulnerabilities, particularly with regards to Taiwanese critical infrastructure and U.S. military reliance on the NIPRNET, but is also partially predicated on a set of misunderstandings, misperceptions, and exaggerations of both U.S. logistics operations and the efficacy of PLA information operations. This final section assesses the balance of these perceptions and misperceptions, concluding with an evaluation of the cost-benefit calculus for the PLA in undertaking such an effort.

Chinese Strategies Against U.S. Logistics Systems and Operations

The Chinese are correct to point to the NIPRNET as a potential vulnerability, but would such an attack actually produce the desired effect? First, there is the issue of the "ready" carrier battle group at Yokusuka, which is only a few days steam away from Taiwan. Though extended re-supply might be degraded, the group’s arrival time would not be heavily affected by attacks on the NIPRNET, undermining a strategic

goal of the attacks in the first place. In response, PLA analysts point to times in the last several years when there was no ready carrier in the Pacific because it was “gapped” in the Mediterranean or in the Persian Gulf. More recently, PLA analysts took note of the DOD's formal revision of its strategy from 2 MTWs to 1 MTW. In both cases, they could envision scenarios in which US forces would require seven or more days to arrive near Taiwan, potentially providing China with a "window of opportunity" to carry out rapid coercive operations against Taiwan.

Second, there is the issue of Chinese characterizations of the U.S. logistics system itself. The Chinese tend to overemphasize the U.S. reliance on computers. The writings of some Chinese strategists indicate that they believe the U.S. system cannot function effectively without these computer networks. Moreover, PRC strategists generally underestimate the capacity of the system to use paper, pencil, fax and phone if necessary. In fact, interviews with current logistics personnel suggest that downtime on these systems is a regular occurrence, forcing US logistics personnel to periodically employ non-computerized solutions. At the same time, there is also evidence that U.S. logistics systems are moving toward increasing automation, which would increase the potential impact of an attack against the NIPRNET.
Third, Chinese analysis seems predicated on questionable assumptions about American casualty aversion, particularly the notion that U.S. forces would not deploy to a Taiwan contingency until all of the assets were in place. If logistics delays meant that some part of the force protection package would not be available, they assume, then U.S. forces would wait until they arrived before intervening in the conflict. This is a debatable assumption, particularly given the precedence of the two CVBG deployment in 1996 and Washington’s considerable interests in the maintenance of peace and stability in the Strait.

Could the Chinese Actually Do It?

In terms of courses of action, interviews and classified writings reveal interest in the full spectrum of computer network attack tools, including hacking, viruses, physical attack, insider sabotage, and electromagnetic attack. One of the most difficult challenges of this type of analysis is measuring China’s actual computer network attack capability. In rough terms, a computer network attack capability requires four things, three of which are easy to obtain and one of which is harder. The easy three are a computer, an Internet connection, and hacker tools, thousands of which can be downloaded from enthusiast sites around the globe. The more difficult piece of the puzzle to acquire is the operator himself, the computer hacker. While individuals of this ilk are abundant in China’s urban centers, they are also correctly perceived to be a social group unlikely to relish military or governmental service.

The answer may be found in the rise of “patriotic hacking” by increasingly sophisticated, nationalistic hacker groups. As demonstrated by the "hacker wars" that followed former Taiwan President Lee Teng-hui's announcement of "special state-to-state relations," the US bombing of the Chinese Embassy in Yugoslavia, and the EP-3 crisis, patriotic hacking appears to have become a permanent feature of Chinese foreign and security policy crises in recent years. One the one hand, the emergence of this trend presents the PRC military and political leadership with serious command and control problems. Specifically, uncontrolled hacking by irregulars against the US and Taiwan could potentially undermine a PRC political-military coercive diplomacy strategy vis-a-vis Taiwan and the United States during a crisis. Unlike traditional military instruments such as missiles, many of the levers of computer network operations by "unofficial means" are beyond the control of the Chinese government. This could negate the intended impact of strategic pausing and other political signals during a crisis. Yet at the same time patriotic hacking offers several new opportunities for the PRC. First, it increases plausible deniability for official Chinese CNA/CNE. Second, it has the potential to create a large, if unsophisticated set of operators who could engage in disruption activities against US and Taiwan networks. One classified PLA document obtained by Taiwan intelligence emphasizes the use of the "unofficial power of IW" and highlights the role of non-state actors in achieving state coercion goals.

For these reasons, some Western analysts have been tempted to assert that the patriotic hackers are "controlled" by Beijing. Among the arguments marshaled to support this thesis is the fact that consistently harsh punishments are meted out to individuals in China committing relatively minor computer crimes, while patriotic hackers appear to suffer no sanction for their brazen contravention of Chinese law. Other analysts begin from the specious premise that since the Chinese government "owns" the Internet in China, therefore patriotic hackers must work for the state. Still others correctly point to the fact that a number of these groups, such as Xfocus and NSFocus, appear to be morphing into "white-hat" hackers (i.e., becoming professional information security professionals), often developing relationships with companies associated with the Ministry of Public Security or the ministry itself. Yet interviews with hackers and officials strongly suggest that the groups truly are independent actors, more correctly labeled "state-tolerated" or "state-encouraged." They are tolerated because are "useful idiots" for the regime, but they are also careful not to pursue domestic hacking activities that might threaten "internal stability" and thereby activate the repression apparatus. Indeed, most of the groups have issued constitutions or other organizing documents that specifically prohibit members from attacking Chinese web sites or networks.

Even if it is true that patriotic hacker groups are not controlled by the state, Beijing is still worried about the possible effect of their behavior in a crisis with the United States and/or Taiwan. Analysis of several recent "hacker wars" over the last two years suggests an evolving mechanism for shaping the activities of "patriotic hackers." In August 1999, after the conclusion of the cross-strait hacker skirmish that erupted in the wake of Taiwan President Li Teng-hui's declaration that the island's relationship to the mainland was a "state-to-state relationship," a *Liberation Army Daily* article lauded the "patriotic hackers" and encouraged other hackers to join-in during the next crisis with Taiwan. In April 2001, *Guangzhou Daily* reprinted without attribution a *Wired* article on the impending outbreak of a "hacker war" between Chinese and American hackers, which many hackers saw as a sign of government backing. A media-generated hacker war thereafter ensued, with Chinese and American hackers defacing hundreds, if not thousands, of web sites. In May 2001, however, an authoritative *People's Daily* article rebuked both Western and Chinese hackers, calling activities by both sides "illegal." This signaled to the hackers that the state had withdrawn its sanction of their activities, and hacker activity quickly tapered off in response to the warning.

A year later, patriotic hacker chat rooms were filled with discussion and planning for a "first anniversary" hacker war. In late April 2002, on the eve of the proposed conflict, *People's Daily* published another unsigned editorial on the subject, decrying the loose talk about a hacker war and warning of serious consequences. Participants in the hacker chat rooms quickly recognized the signal, and the plans for a new hacker war were abandoned. In neither case could this dynamic be called control, but instead reflects the population's keen sensitivity to the subtle messages in government propaganda, which continues to successfully create a Leninist climate of self-deterrence and self-censorship that is more powerful than active state repression. As some groups move into "white-hat" positions, however, the relationship might actually transition from a ruler-ruled dynamic to a partnership motivated by reasons ranging from nationalism to naked self-interest.

A final issue related to measuring capability involves the assessment of a group or country's ability to generate new attack tools or exploits. Outside analysts, many of whom are programmers themselves, tend to reify countries like Russia that abound with highly talented programmers, and look down upon countries or individuals that simply use off-the-shelf "script kiddie" tools like distributed denial of service (DDOS) programs. DDOS is admittedly a blunt instrument, but a fixation on finding more sophisticated attacks, which reflects the widely-held but logically tenuous assumption that state-sponsorship correlates with sophistication, may be counterproductive. Instead, analysts should employ a simple "means-ends" test. In the Chinese case, DDOS, despite its relatively simplicity, looks like the right tool for the right mission. From the Chinese point of view, for example, hammering the NIPRNET and forcing it to be taken down for repairs would be considered an operational success, since it could potentially delay or degrade U.S. logistics deployments to Taiwan.

In conclusion, therefore, a strategy to disrupt U.S. logistics systems with computer network attack seems well-matched to U.S. vulnerabilities and Chinese capabilities, though the final operational impact of the effort may be undermined by important Chinese misperceptions about political will and the nature of U.S. logistics operations.

Panel III: Discussion, Questions and Answers

HEARING COCHAIR BROOKES: Thank you.

I have a few commissioners with questions. I'm going to start. I open this up to the panel, whoever would like to respond. Do we have any sense of the amount of resources in terms of personnel, schools, budget, that China is devoting to cyber warfare?

DR. MULVENON: It is interesting. There is a tremendous amount of information available about certain institutions in China. I think we have a very good understanding within China of which institutions are involved in cyber warfare-related R&D, particularly good understanding of where it happens within the professional military education framework, places like the Wuhan Communications Command Academy, whose curricula came into our hands through open sources at one point.

Again, I share Tim Thomas' view that the level of detail and sophistication in that curriculum was actually quite astonishing. Certainly changed our assessment of where we thought the Chinese were in terms of sophistication.

But I would simply caution that we often get into a game with China of sort of thousands and thousands, there are 50,000 Internet police, there are 50,000 Chinese military hackers being trained, when in fact I would argue, and perhaps this just reflects my own misspent youth as a computer hacker, that a very small number of people operating in a highly secure compartmented way can have a pretty devastating effect, and I'm not terribly interested in how many zeroes there are after the number of personnel that are involved in it.

The Chinese write about how they want this to be a carefully controlled national activity. I think there's a lot of misinformation on the street about Chinese information warfare militias operating in rural areas conducting computer network attack.

I think there's a lot of misunderstanding about some of that data, but from a resource perspective, we do see a very robust, for instance, R&D funding effort underway under portions of the 863 Program and other national defense S&T programs, to be able to fund on the technical side as well as the technique side and even on the defensive side to improve the Chinese military's ability to conduct computer

network operations.

HEARING COCHAIR BROOKES: Mr. Thomas, do you have anything to add to that?

MR. THOMAS: Yes. One of the questions we're often asked is what's the purpose of all these numbers? Like James has said, you know, we hear the 30,000, the 50,000 all the time. I think the last I heard on computer hackers was 250 groups. People have asked is this part of their information deterrence theory as well? By getting us to think there are so many people or groups involved there, that we then overestimate their capabilities and, in fact, then become part and parcel of their information deterrence undertaking.

So I would have to go along with what James said on that because it's quite stunning when you look around at the number of groups that they profess to have all the time.

The other thing that was interesting, since James mentioned the Wuhan curriculum, the other thing that was interesting to me from the curriculum here was the course titled "An introduction to U.S. and Taiwanese social information systems." Taiwan and the U.S. were the only two countries mentioned in all of these four semesters of courses. A reference to social systems means they may be looking at things like Facebook and others as well.

So the recruiting effort or the ability to get in and manipulate or find what some young person who is connected to someone on this Commission might be thinking, you know, there's other areas here where they may be probing as well. That's about all I would have to add.

HEARING COCHAIR BROOKES: I have one quick question. Do we, when we talk about computer network operations or activities, have we given much thought to what constitutes aggression or hostility?

I open that up to the panel as well.

COLONEL McALUM: I think that gets back very much to the point of discussion on lexicon, getting that right. For us, from the Department of Defense perspective, when something becomes disruptive, I think you start to get into the point where that action could become something called an attack or maybe not even disruptive in the sense that we're going to deny service, but if you begin manipulating information or cause a loss of confidence in your information or your information systems, I think we would start to get into an area that we would have to talk about being, again from a disruptive perspective, something much more fits that model versus the data mining, data collection, reconnaissance things we've been talking about.

MR. THOMAS: I could add a little bit here from a Russian

perspective that ties into the Chinese, and that is the focus of what's going on in Russia right now. They are seriously looking at how to define information aggression, information territory. I know this morning you had a brief discussion about territory.

The Russians make a point that they're linking up with the Chinese and the Shanghai Cooperation Organization and other areas where they're talking about these issues, and I don't know who within the State Department is part of that discussion, but I would hope that they stay in touch with this issue, because it is important to find out where these issues are being taken by the international community.

In fact, with Russia, I would say that that is one of their bigger goals, to shape that argument.

DR. MULVENON: Commissioner, you raise one of the key issues that's so difficult to talk about in this area. The Cyber Conflict Studies Association for the last year has been running a series of workshops on cyber deterrence and trying to apply the tools of Tom Schelling and Herman Kahn and others, you know, "the greats," to this problem, and finding, much to our frustration, that many of those tools, those strategic concepts, those strategic principles, fall down with the technical realities of cyber warfare, and particularly the attribution problem we're finding undermines many if not all of the pillars that we've come to rely on.

If you don't know who is attacking you, then it's very difficult to be able to figure out how to respond. If you can't be guaranteed of effect, which is a problem with computer network attack, then you can't develop either proportional or disproportional response and rely on it in the way that we could rely on the effects of nuclear weapons 1977 and the wheel of death to assure us that this amount of pounds per square inch of overpressure was going to do the following to the following type of building.

In that kind of realm, figuring how we possibly could either deter or compel and where that line of aggression is, given the difficulties we have with attribution, becomes very, very difficult, particularly if, as I said, you consider a scenario in which the Chinese initiate the attack, for instance, within CONUS. How is that defined?

HEARING COCHAIR BROOKES: This question came up recently with the denial of service attacks on Estonia. The defense minister, if I remember correctly, talked about invoking Article 5 of NATO. So this is a big question, this question of escalation, moving from non-kinetic to kinetic. But these are some things we should be thinking about.

Commissioner Blumenthal.

COMMISSIONER BLUMENTHAL: Thank you. I'm Commissioner Blumenthal and I too have been a victim of Chinese

cyber crime in the interest of full confessional, and I have an appetite for vengeance myself, but I'm sublimating it.

There are certain concepts--I'm looking for the right analog and I asked this of the space people earlier today--and the Colonel mentioned today this question of an intrusion into an Air Force base versus an attack on an Air Force base, mentioned the words "electronic dominance in 2050."

Dr. Mulvenon mentioned the Cyber Conflict Studies Association with all the analogs to earlier RAND studies of deterrence. But--this is a question I asked of the space people too--in a wartime situation, is it even possible for the United States to gain supremacy or dominance or superiority over the electromagnetic spectrum? Or anyone to actually gain dominance over it in a way that we would want to in other domains to conduct operations?

And what do the Chinese mean by electronic dominance in 2050? Two related questions.

COLONEL McALUM: Well, it's a great question, sir, and our depending on the type of electronic and network systems that require the medium that we're talking about here, it's a significant challenge. I'm sure you heard about our concerns about jamming of satellite communications as well as other space-based capabilities.

When you roll in the ability to disrupt the flow of bits and bytes and information across data networks, whether those are deployment orders or spare part orders or whatever, or the flow of imagery from UAVs in over one part of the world back to the states, I think that the concept of electronic magnetic dominance means the ability from an adversary's perspective is to prevent our use of those capabilities or significantly hinder our full ability to use it to our benefit.

I'm not sure that any adversary could expect to lay total claim to any of those mediums and at the same time deny our use of it. So I think it's a case of those how much can they disrupt our ability to take advantage of it and add disruption into our systems and processes versus somehow lay claim and dominate it as we would the airspace over a particular target.

COMMISSIONER BLUMENTHAL: What about ourselves? Can we dominate, if we wanted to, in wartime? Is that even something that's attainable, the dominance of the electromagnetic spectrum?

COLONEL McALUM: I would feel more comfortable talking about that one offline or taking it for the record.

DR. MULVENON: I would simply offer a slightly different perspective as well, which is to say that in a recent offsite I attended for OSD, that was looking at this cyber deterrence issue, it was posited that we shouldn't trap ourselves into thinking about cyber-for-cyber,

electronic-for-electronic, but we should, in fact, begin with the premise that we have all of the tools of the full spectrum of U.S. national power, and that in many cases, it may not be to the U.S. advantage to respond to an electronic or a cyber intrusion or cyber attack simply in that realm, but that we may in fact want to take advantage of escalation dominance that we have in other elements of national power, whether it's military or economic, and that we should look at that toolkit the entire time.

And so while there may be a problem in the electronic area, the best way for us to repel that attack or to compel it to stop would be in other areas of national power.

As for the Chinese definition of electronic dominance, I find them to be quite confused and scattered on the issue. I've read everything from it being defined as simply being able to carry out area or access denial, electronic dominance in a certain area close to China's borders around Taiwan in terms of electronic warfare dominance.

I've seen it described within the informatization literature as China is pushing its own variance of all of the world's information communication protocols, using their market access as leverage to foist basically VHS upon a Betamax world, to bring inferior standards, because so much of the equipment is made in China, to infrastructure dominance.

There's a large debate about what percentage of the submarine cables in the Pacific are actually controlled by Chinese or Chinese-affiliated entities and whether that infrastructure dominance could be leveraged in wartime. So I think it works at a lot of different levels.

COMMISSIONER BLUMENTHAL: But just to pursue this question of when you look at China and the anti-access threat, in war time, when it comes to air defenses and so forth, and anyone taking on China in a conflict would want to suppress those, would we have the same capability to suppress attacks on our ability to operate within the electromagnetic spectrum from radio frequency to NIPR and SIPR?

Again, is that an attainable goal on our part as, let's say, suppressing an air defense system would be? Is that a correct way to even think about it?

DR. MULVENON: I agree that our specific capabilities in that area are probably best discussed offline, but I would just simply highlight a key difference between the Chinese and U.S. systems, which is that as is well-known, more than 90 percent of our critical infrastructure, upon which a lot of our unclassified capability in particular rides, is in private sector hands, whereas in the Chinese case, the infrastructure backbone that they operate on in interior lines is quasi-public.

And so the extent to which that's leverageable in a wartime scenario or, to use the correct Chinese phrase, to be able to be mobilized in a Taiwan scenario is a fundamentally different structural aspect of our two countries.

COMMISSIONER BLUMENTHAL: Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Wessel.

COMMISSIONER WESSEL: Thank you for being here. It's a fascinating subject, and as you pointed out, having read a 2001 CRS report, I'm sure that we will continue to be dealing with this topic for quite some time.

I'd like to challenge the notion of perimeter security in a way and going off of Mr. Thomas, who had a number of sayings, it sounds to me like the Chinese are speaking softly but selling us their big stick.

We saw Lenovo two years ago trying to sell roughly a thousand computers especially designated for the SIPRNET at the State Department. Ultimately, that sale did not go through.

If you look at Cisco and many other router companies and others, much of the infrastructure, much of the perimeter you talked about, is, in fact, being produced offshore and a significant amount of that increasingly in China.

I saw press reports earlier this year, that there were up to 300,000 hard drives that had been returned to an Asian country for concerns about whether there was imbedded software in those hard drives or in the BIOS, as I recall. Should we be looking at a different definition? Can we, in fact, have a secure perimeter if, in fact, the Chinese are helping to build that perimeter?

COLONEL McALUM: I'll start off on that one, sir. I would agree. I'm not sure you could put a lot of stock in building a secure perimeter. I don't like to think of it so much as a fence as rather more as a filter. And so from a DoD perspective, we see the perimeter as an opportunity to filter out some noise.

We talked about the significant increase in malicious software and activity on the Internet, so from our perspective, today we let a lot of that in our perimeter for technological reasons of how it was architected from the beginning.

Based on some of the capabilities that we have in place and are deploying, and not all of that is necessarily commercial off-the-shelf technology, we see an opportunity to start filtering down and reducing what we call the white space in order to focus on those more serious problems that will undoubtedly pass through.

Again, the idea of a fence, agreed. I don't think that's something that we look at it from a perimeter security perspective, more as an

opportunity to filter, and we are concerned about the type of infrastructure that would be in place.

COMMISSIONER WESSEL: But from a global sourcing perspective and going off of the PC World or PC Magazine, things that are commonly known, not all open source, you have remotely-triggered viruses, remotely-triggered exfiltration devices, et cetera. Much of that can be built into the hardware, the chips, et cetera. As I recall, we have one trusted foundry and that's for hardened chips, not for designing software control chips.

What are we doing about the globalization of the supply chain for this perimeter because it's not secure, just as you described. There could be, in fact, latent problems that can be triggered later on.

COLONEL McALUM: You've asked a tough question, from a supply chain perspective in a globalized economy, very, very difficult. I can only speak from the Department of Defense perspective. Much of what we deploy, and again, I'll just talk in generalities here, from software, enterprise software capabilities, and some of the infrastructure that we're deploying, we put a lot of emphasis on trying to understand where it came from and who's touched it.

We can't do it all, but we put again, from a risk management perspective, you put more emphasis on certain parts of your infrastructure than others, but it's a very big challenge in a globalized world.

COMMISSIONER WESSEL: Either of the other witnesses?

DR. MULVENON: Commissioner, I would obviously agree that supply chain is a big problem, particularly given the increasing percentage of these products that are being manufactured in China, the pressure that's being put on some of these companies to include Chinese standards, which involves giving up source code for Chinese-designated companies to then be able to build the APIs to make them compatible with those Chinese standards.

But, we should also look closer to home as well as in the sense that, as a Mac user since '87, I can tell you that Microsoft and its buggy code probably represents a far graver information warfare threat to the United States than a lot of backdoor Chinese equipment. But as long as we have a low bid acquisition strategy in that area, we're going to go down that road, and it requires much more attention to code auditing and hardware auditing than we do right now.

I think people are only beginning to realize the imbedded vulnerabilities that we have because of those supply chains and I think a lot of the recent changes in the export control regimes are a reflection of people's concerns about that. But it's not moving nearly as quickly as I'd like.

COMMISSIONER WESSEL: Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Fiedler.

COMMISSIONER FIEDLER: I'd like to get back to the attribution problem. It strikes me that attribution is a problem in peacetime and less of a problem as we are approaching conflict because there would likely be other activities and information available to us to indicate who the culprit is. Am I wrong?

COLONEL McALUM: That's a great point. I want to differentiate or add a little bit to what was previously discussed on attribution. So there are really two aspects of attribution. There's a technical attribution problem which is what's the last box of origin or where is the box physically located? The box might be located on an educational network or a commercialized P in some other country, but then there is the problem of actor attribution, whose fingers are on the keyboard. And that gets into who's causing that box to be a problem for you, and they may be sitting somewhere else.

Then, you have to understand intent and so forth. So actor, the technical attribution and the actor attribution are different, and one may be easier to determine than the other, and in a crisis situation or a ramp-up to a crisis situation, I would only talk in generalities, that certainly there would be a lot more emphasis on intelligence, indications of warning, and other assets that might be able to help speed up that process, but identifying technical attribution is one problem. It may happen quicker than the other part of the actor and intent and so forth.

DR. MULVENON: I would agree with that completely. I think there would be a lot of other indicators and warning in a crisis in a wartime situation. I would say, though, from my own personal experience, even looking at the intrusion forensics against my own personal systems rather than the work we've done with the Department, that from log data alone, it's very, very difficult to figure out what's going on because all you see is that last hop.

The software is usually a cut- and-paste pastiche of a thousand different authors, but I will say that in the absence then of compelling smoking gun evidence, we often sit back and we say to ourselves "cui bono," who would benefit from this sort of thing? Your average hacker is very interested in credit card numbers, they're very interested in buying and renting botnets to organized crime and a number of other things.

They tend not to be as fascinated with mind-numbingly boring NIPRNet configuration files published by Transcom. So in that situation, I tend to ask myself who in the world would be interested in this sort of thing? And there, suspicion often moves to the people who explicitly write about the extent to which NIPRNet and those types of

unclassified systems that run logistics information on them would be prime targets in a wartime scenario.

It may not be the Chinese government itself that is doing it. It may be proxies. It may be, as we've seen in the China espionage world, what I call espionage entrepreneurs, people who acquire things and then go looking for a customer for them. They may not be directed to acquire that information, but they know that it has value, and then again in addition to who benefits, it's where does it end up and who could it possibly benefit?

So in the absence of technical attribution, which is a very difficult problem that's endemic to the nature of the way the Internet is architected and has been architected for its history, we fall back on more social elements and trying to understand motivation and intention.

COMMISSIONER FIEDLER: Thank you. Another question on critical infrastructure. We've talked a lot about intrusions into government networks. What about intrusions into our critical infrastructure and the relationship that our government has with our private sector providers of power?

COLONEL McALUM: I'll just add a little bit to that one. I would tell you that Department of Homeland Security would be the best to discuss that in detail. I will tell you from my own knowledge that there has been a certain amount of activity and effort working with industry and the Department of Homeland Security and law enforcement to take a look at vulnerable systems that are supporting our critical infrastructure to include SCADA-like systems, Supervisory Control and Data Acquisition systems, very important to a lot of our industrial operations.

I would also point out anything that's connected to the Internet, that's accessible from the Internet remotely, is potentially vulnerable. And so there is a lot of concern about what might those type of systems out there today that are many times built, stovepipe systems built over time, legacy systems, that may not have been built with security in mind, how vulnerable might they be to some types of cyber compromise?

So a lot of effort I think has gone into that and I would just point you in the direction of the Department of Homeland Security I think for more information.

COMMISSIONER FIEDLER: Anybody else? Thank you.

HEARING COCHAIR BROOKES: Thank you. Commissioner Reinsch.

HEARING COCHAIR REINSCH: Thank you. I wasn't going to get into this, but since Commissioner Fiedler raised it, let me pursue that last line for a minute. Dr. Mulvenon, you might want to have a

comment as well as Colonel McAlum.

Critical infrastructure in the private sector is something I worked on when I was in the Clinton administration where we tried to get the relationship between the government and the private parties organized so the latter could do a better job of protecting themselves.

My impression just from open sources and media is that things haven't progressed all that much in the last ten years. Am I wrong about that?

DR. MULVENON: Well, sir, I would say that in part there's a number of thorny issues that you're very well aware of, particularly the liability problem. In the conference we had in February at Georgetown on the Estonia attacks, we had a panel devoted to the private sector, and they were as scared as cats in a rocking chair factory to talk about the extent to which they should be held liable for either helping or not helping the government identify blue versus red packets because they said we can do that, but are you going to protect us on the liability side?

I think the unspoken message was we went down that road with the alleged terrorist wiretapping program and don't like where that led, and so the idea that we're going to get on board again of the potentially high liability situation involving critical infrastructure protection against cyber attack, you know, met with a lot of skepticism.

I think that that private sector partnership, I think there's a great amount of dissatisfaction on all sides with the current situation with the infrastructure vendors basically saying for our own market-related reasons, we're going to take care of our own network and we don't really want to be involved in some larger scheme. I think that's the real point of tension.

HEARING COCHAIR REINSCH: Colonel McAlum, I saw you get an infusion of wisdom there. Do you want to add anything?

COLONEL McALUM: No, sir, I have nothing to add. Thank you.

COMMISSIONER BLUMENTHAL: That was the wisdom.

COLONEL McALUM: Lawyers.

HEARING COCHAIR REINSCH: That may have been the best advice you've gotten all day.

Going back to Dr. Mulvenon, then that suggests that the best thing the government can do is nothing.

DR. MULVENON: Well, I don't think the best thing to do is nothing. I think that there is a place--I'm not, I believe in the free market. Let me put it that way. But I do believe that certain standards within the free market of quality of service can be guaranteed still within a market context, and particularly when we're looking at these

critical infrastructure providers going global.

I know we've had a number of nasty tussles about CFIUS and Chinese purchase of various things. But this is going to be nothing compared to when the China Investment Corporation and its $400 billion worth of foreign exchange comes shopping, particularly for infrastructure, and we're going to have a lot of questions about that because I don't think we can imagine a future in which all of the infrastructure is owned by blue even within the continental United States.

And so what do we do in that situation in terms of government cooperation, particularly with a foreign owner of infrastructure?

HEARING COCHAIR REINSCH: We'll send them to your company when they come shopping. It might provide an opportunity.

DR. MULVENON: Yes, cash only.

HEARING COCHAIR REINSCH: RMB or dollars? Colonel McAlum--actually any of you, but Colonel McAlum in particular--when Representative Lofgren was here this morning, she made reference to one of the perimeter defense issues, which has been publicly reported, as reducing the number of Internet portals, access portals. And we then had a brief conversation about whether that was wise or not and what some of the down sides of that are.

Can you explain in a little bit greater detail why that's a good idea and what some of the consequences might be?

COLONEL McALUM: Sure. From an operational perspective, decreasing the number of access points in and out of your network is a very good thing especially if you put the right sensors in and improve your situational awareness and your ability to do something about it. I think the open source reporting said there's literally tens of thousands of access points in and out of government networks. That’s a huge number to try and monitor from a situational awareness perspective.

In the Department of Defense, we have 17 Internet access points between the NIPRNet and the Internet, and we're decreasing that number.

Those are huge interaction points and again depending on the type of technology we deploy at those sites, our situational awareness of what's coming and going could be very, very useful. We obviously wouldn't want to decrease it to a number that becomes a liability in the sense of chokepoints, but I think there is a right balance there.

So tens of thousands is probably too many and very hard to control from a governance perspective, and one or two is probably way too few from a reliability/redundancy perspective, but there's a lot of reasons to do that, and getting a handle on your enterprise, you have to decrease the number of those entry points and control them.

HEARING COCHAIR REINSCH: Would you put the number now

in the tens of thousands?

COLONEL McALUM: What's been reported in the open press is that there's tens of thousands of connections between government networks and the Internet.

HEARING COCHAIR REINSCH: I just think it eliminates redundancies and creates some vulnerabilities, but your point is well-taken. Maybe I'm thinking of when it's one or two, but I take your point. Thank you.

HEARING COCHAIR BROOKES: Thank you.

DR. MULVENON: Commissioner, what you need to understand about that just briefly is the dot.gov domain is not centrally managed. It's been managed on an ISP by ISP basis, and the proposal is to centrally manage the dot.gov domain so that you could then have those kinds of access points, but right now there is no ability to actually centrally manage it.

HEARING COCHAIR REINSCH: Yes, thank you. I guess I'm questioning whether that's a good thing or not, but we could have that discussion later.

HEARING COCHAIR BROOKES: Thank you. Commissioner Mulloy.

COMMISSIONER MULLOY: Thank you, Mr. Chairman. Do we have domestic laws that prevent companies from cyber attacking other companies? DR. MULVENON: Yes, sir, I'm intimately familiar with it. It's the 1986 Computer Fraud and Abuse Act, which argues that any unauthorized intrusion into another person's server is illegal, and that includes servers abroad because obviously when you're a U.S. person and you're acting abroad, you're still governed by U.S. law.

And so that is the operative law. It's been revised many times to reflect changes in technology and everything else, but it also governs--it also is the law governing our ability potentially to conduct computer network operations abroad and the need for presidential covert action findings and the like.

COMMISSIONER MULLOY: Okay. So we've found a way to try and control this domestically insofar as domestic companies maybe doing it to one another?

In one of our briefing papers for this hearing, there's an article from the Christian Science Monitor, dated September 14, 2007, "China Emerges as Leader in Cyber Warfare." And then the article goes on to say that China is hardly the only state conducting cyber espionage. Everybody is attacking everybody.

Then the article goes on to say that German Chancellor Angela Merkel raised the issue of cyber attacks on her country from China with Chinese Premier Wen Jiabao, and then it goes on to further state

that President Bush raised the issue with President Hu Jintao when he met with him in Australia, pointing out that computer systems, respect for computer systems is, quote, "what we expect from people with whom we trade."

I go back and I think about international environment, when pollution came from one country and began to impact on another country, and people said, well we ought to control this, so we had a conference, First U.N. Conference on the Human Environment, in '72, and then legal principles began to emerge and we tried and now we build on those.

Why is there not an effort in the international community, instead of spending all this money defending ourselves, why don't we get a treaty that bans this kind of stuff? And do it that way and put it on the obligation of the state to control its own people, the way presumably we do, at least domestically?

DR. MULVENON: There is some interesting thinking in this area. I would refine your thinking a little bit in the sense that the thinking is that you would hold countries responsible not for the actions of their people, since the attribution problem prevents us from actually attributing that a Chinese person or a Romanian person actually did something, but making a country or service providers or infrastructure providers responsible for the packets exiting their network.

And that networks and infrastructure that don't adhere to those rules are then denied privileged peering access into other networks. So it creates a market dynamic whereby if you want to continue to have peering and interconnection access to other networks around the world for your business model, you need to then self-police yourself to be able to make sure that hostile packets are not leaving your network.

COMMISSIONER MULLOY: What do you other two think with the idea he just proposed? Is that a good way to go?

COLONEL McALUM: I think it's a great way to go. It's not the only solution to a problem, but going back to the service providers themselves and putting more of the onus on them is a great idea.

If I have an MSN account like I do at home, I do get malware at home, and if I don't have my defenses on my computer set up, I'm infected and I'm compromised. But at the same time, MSN has no liability for that. So if they are going to provide a level of security that I would expect they're probably going to charge for it, and I'm willing to pay for it.

So they're going to have to put the tools and the capabilities in place to be able to provide that. I think the model he's talked about is a rough parallel to what happens in the air traffic control business. If an airport doesn't measure up to certain security standards, okay, for

whatever reason, either they failed an inspection or there's been an incident there, that airport will not be suitable for landing rights until they fix their problems and so they will not be allowed to be part of the international air traffic control system.

Same sort of concept. If an ISP or any sort of provider, whether it's a dot.edu or a dot.com or a dot. whatever, is a source of the problem because they're not policing up their traffic, you know, one way to enforce that would be you're not part of the Internet community till you solve your problem. So very simplistic approach, but there's a lot to be said for that.

COMMISSIONER MULLOY: Just one last question. Is there any effort within this administration to lead an international effort to try and get some legal treaty or effort to stop this type of behavior?

DR. MULVENON: Well, sir, the State Department under the capable leadership of people like Michele Markoff for many, many years conducted international critical infrastructure protection coordination meetings with countries around the globe seeking in a systematic interagency/interdepartmental way to harmonize domestic laws in other countries to make it easier for us to extradite people, to be able to prosecute people.

And that effort is ongoing, and I think there were some real successes in that area, particularly with allies, and you saw that in the Estonia case in terms of the kinds of coordination infrastructure that had been built between like-minded countries to be able to participate in these things together, yes.

COMMISSIONER MULLOY: Thank you very much.

HEARING COCHAIR BROOKES: Thank you. I think we're going to start a second round of questioning if we could.

I have a couple of quick questions, and I open this up to the panel. Can we expect any indications and warning, strategic indications and warning of a cyber attack? Or is it basically a bolt from the blue without any warning? Is there anything that, in terms of conventional warfare-- we often have indications of warning of a potential attack or imminence-- would have in terms of cyberspace?

COLONEL McALUM: It's hard to draw the parallel to the kinetic world. You know in the nuclear business you see the missile being moved to the launch pad, it's being fueled, it just left the pad, it's 15 minutes out, here's where we think it's going to impact, etc., etc. You know that's a serial process in the kinetic world.

In the cyber world, you don't necessarily get the notification, well, the zero day exploit has just been loaded on a computer, he's about to hit the send button, here it comes, here is where it's going, etc., etc.

The time variable is the biggest thing that probably discounts

that in many ways. Again, we would expect that many different forms of intelligence would be supporting the indications of warning in a pre-crisis or a build-up to an event, but zero warning, start to finish, in the millisecond world that we live in on the Internet, that could be very difficult to attain, but we'd like to believe that we'd have a good sense of something bad happening and be able to at least focus the right assets toward that.

HEARING COCHAIR BROOKES: So it's issues outside of cyberspace? In other words, you're saying an issue such as political tensions would be an indication, but that we may have none in cyberspace?

COLONEL McALUM: I'm not going to say we don't have these. I'm just saying it might be a challenge.

HEARING COCHAIR BROOKES: Okay. Would anybody else like to weigh in on that?

DR. MULVENON: I would just say that one of the interesting insights from the Chinese literature where I think in many ways they may be ahead of us about this is when they often argue that a computer network attack will by necessity be a bolt from the blue, particularly against a high tech enemy, because that's the only place that you can get an advantage, and that you have to do very meticulous computer network reconnaissance to be able to assess the vulnerabilities for that.

People can disagree about whether you would have a confidence level in carrying out that kind of attack simply with passive network reconnaissance or whether you actually need to reach out and touch things.

But what the Chinese military argues in its internal writings is that that's all you're going to get, is the bolt from the blue, because unlike in our system where we potentially see it as a force multiplier at every stage of Netcentric warfare, because of the fact that all of that network reconnaissance will then go out the window, because the adversary will either then patch the target set, take the target set offline and unplug it if you can if it's not mission critical.

But whatever is going to happen, you have a much lower level of confidence you can communicate to your leadership that in real time against an adversary that has full shields up, 24-hour alert, that you're then going to be able to find new fresh zero day vulnerabilities against that network with which to exploit, or that you're even going to be able to use the potential malware that you have imbedded in the system because of the nature of the network.

And so they argue the bolt from the blue is really to kneecap the high-tech adversary at first, but not necessarily be able to conduct those attacks throughout the whole course of the conflict.

HEARING COCHAIR BROOKES: Mr. Thomas.

MR. THOMAS: Taking a little different approach on this, if you were looking at what they're saying internally, they're also saying we don't even want the other side to know that a bolt from the blue happened, that there would be no indication and warning. The example that they give quite often is, “how do you make a cat eat a hot pepper?”

And they relate that “you can jam the pepper down the cat’s throat, you can wrap it in cheese, or you can crush it, spread it on its back and let the cat lick itself.” This self-accommodating idea is strategy, that you got the cat to do what you wanted it to do without the cat realizing what had happened.

So this whole self-accommodating idea fits very well within that bolt from the blue. The Chinese do talk about the fact that reconnaissance offers you the ability to take the initiative, and more the ability, like Jim was saying, to know where those holes are and the vulnerabilities. But that's just a little bit different take on what they had to say.

HEARING COCHAIR BROOKES: Are we going to see reconnaissance? How does a cyber attack evolve? Would we see reconnaissance first? Is there something or is that not necessary?

COLONEL McALUM: I would say sure, you might see some scanning take place. I would tell you that's going on all the time. It's high volume every single day, not just against DoD but throughout U.S. government.

I would also tell you there's a lot of things you can discover without ever penetrating another person's network. Those vulnerabilities, you could do a lot of research on your own open source to discover vulnerabilities that could be exploited at another time.

As previously mentioned, I would reiterate there's an underground market for zero day vulnerabilities that can be sold and then stockpiled for later use. So reconnaissance could be one form of some sort of indications and warning. You probably wouldn't see it in the noise level that we're dealing with today, but you might, so I would just say there's multiple ways to gain insight that something is about to happen.

HEARING COCHAIR BROOKES: Anything else?

MR. THOMAS: A direct quote from the former Director of the Third Department, the Information Warfare Department: "Computer network reconnaissance is the prerequisite for seizing victory in warfare. It helps to choose opportune moments, places and measures for attack."

And he talks about it quite openly.

HEARING COCHAIR BROOKES: Okay. Commissioner Fiedler.

COMMISSIONER FIEDLER: A couple of things. I'm going to return for a moment to the critical infrastructure question, and since most of you are DoD oriented, let me ask it this way. Is every defense contractor required to report intrusions within a short time period?

DR. MULVENON: Well, sir, as someone who recently in the last three years built 20,000 square foot of defense security service certified space, I can tell you yes. If those defense contractors have in particular contracts with the Department, in particular if they have a security clearance through the Department, they are absolutely obligated under their AIS plan to report any and all of those intrusions.

COMMISSIONER FIEDLER: Within how long?

DR. MULVENON: I couldn't tell you how long it is, but the longer you wait, the more suspicious it looks.

COMMISSIONER FIEDLER: I do know that. Do you know, Colonel?

COLONEL McALUM: No, sir, I can't tell you exactly. I do know that there's an effort underway that's hosted over at the OSD level working with defense industrial base companies to improve the reporting processes that are out there today and hopefully to speed up that process. I can't tell you exactly what the requirement is.

COMMISSIONER FIEDLER: Okay. Then I suspect the answer to my question about whether or not power companies are required to report intrusions to the Department of Homeland Security is probably nonexistent; is that correct? Anybody know?

COLONEL McALUM: Sir, I don't know. I would refer back to Presidential Decision Directive 63. It talks about critical infrastructure protection. There's a series of information sharing and analysis centers across critical infrastructures. I suspect reporting of that type, if it's taking place, would probably come through that channel, which is not necessarily official reporting.

COMMISSIONER FIEDLER: And let me try to put the recon issue into perspective. Everything you've talked about operating at the speed of light here or faster with computers seems to me to make people's reconnaissance somewhat obsolete rapidly, therefore necessitating constant reconnaissance.

Am I missing something here? On vulnerabilities of networks?

DR. MULVENON: Well, no, but there's a real tension there. In different communities within the system, you'll hear people say please don't let your computer network attack operations screw up my computer network exploit operation in the sense that the more computer network reconnaissance you do, the more danger you arouse of the adversary potentially detecting that reconnaissance and patching the very vulnerabilities you were planning on exploiting.

So there's a real cost curve there that you have to deal with, and you don't want to obviate the value of all that computer network reconnaissance that you had just done.

So now, it may, in fact, if you are a smaller power, a less capable power, it may in fact not necessarily be against your interests for the adversary to know you're engaged in that kind of probing because, as Tim said, it may in fact be part of your information deterrence campaign.

It may be designed to keep you guessing about just exactly where people might be in your network and reduce your confidence level in the performance of those networks.

But at the same time if you really want to use it in a warfighting context, that's why these types of activities, if they go on within our system, are very highly classified and compartmented.

COMMISSIONER FIEDLER: Thank you.

HEARING COCHAIR BROOKES: We have just a few moments left so maybe if we could get both Commissioners Wessel and Blumenthal to give their questions and then let them answer, that might be the most expeditious.

COMMISSIONER WESSEL: That's fine. I wanted to follow up briefly on the line of questioning that Commissioner Mulloy, who is gone now for a moment, had raised about possible liability and other issues because there seemed to be some view that imposing the burden on ISPs to look at outbound traffic might be an appropriate way of ensuring greater security on the network.

I think we've seen a problem with that in China where national security has been so broadly defined that the Chinese want ISPs and routing companies to limit the words "Tiananmen," "freedom," and other issues, which has raised concerns here in the U.S.

I'm not necessarily looking at an ISP looking at all of the traffic going into my network or my home computer to review whether there are pixelated viruses or whether whatever standard there is. I think it's actually intended on the user. That's where the liability is.

But there seemed to be some receptivity, I just wanted to raise a question as to whether there are broader issues here we should be looking at in depth?

COMMISSIONER BLUMENTHAL: I also wanted to follow up on some of the legal issues that this new type of conflict might raise, more in terms of operational law and recommendations we can make to the Congress.

It seems like on the spectrum of conflict, reconnaissance and espionage that's going on everyday, as we've heard, there's probably not--you can correct me--I'm making kind of propositions and assumptions that may not be correct--but there's probably not too much

military or operational law that covers those types of activities in terms of the types of responses we can take.

But if you move down the spectrum from denial of service, imaginable hypotheticals, the disruption of electricity in the United States or in allied territory that actually ends up killing or harming people because of the denial of service, that can somehow be attributable to the Chinese, have we developed our operational laws in ways that we would have a framework for response and a way that we can go to the Chinese and say if such and such happens under the laws of armed conflict, we can take a kinetic response in certain circumstances?

And if not, where do we need to develop those areas of law and particularly suggestions we can make to the Congress to pursue those areas of law in this new area of conflict?

DR. MULVENON: I would say that on the ISP burden issue, in many ways, the irony is that the Chinese, we talked about 50,000 Internet police. That's not the secret of Chinese Internet censorship. The secret to Chinese Internet censorship in addition to the very technically capable firewall, which came later, was initially very successful because they wrote an ISP law that said an ISP was simply responsible for the activities of all of its subscribers.

And so what the ISPs did was they hired people to sit in chat rooms and bulletin boards, which is a fate worse than death as far as I could tell, but to just sit there and kick people off who engaged in political content and everything else, and so they pushed the burden down to the ISP level, now, admittedly, used for evil purposes, but a market-based solution nonetheless because what they said they would do is they would put the ISP out of business if it violated that particular rule.

I can imagine one governed by perhaps a bit more of an enlightened principle such as the defense of the United States that might work a little bit better.

On the legal side, Commissioner Blumenthal, there's been a tremendous amount of work done on this over the last ten or 15 years in the Department, but I would still say that there is also still tremendous ambiguity and lack of assurity that the legal frameworks are in place in many cases for this to move forward, but those discussions about where those lines are and what the criteria are and everything else I think are being addressed by the current presidential initiative and are certainly very sensitive.

COMMISSIONER BLUMENTHAL: Anyone else on that?

COLONEL McALUM: Going back to the item on the ISPs, I think it would be a question of degree. I think the general public perception is if ISPs get involved and are liable, I'm going to give up

privacy, and I think it's a question of degree, who's reading my e-mail?

There's certain types of malicious software and packets and attachments that nobody has to open up to figure out they're bad. There are tools that will allow you to scan it and determine it's bad. Why would you ever allow a buffer overflow attack come into the network? You can stop that upstream, not a problem.

Again, I think it's really a question of degree. I think ISPs can be held liable to a certain degree for a certain type or level of bad traffic, and then beyond that, I think we would have to progress and evolve on how much exactly we would want them to be liable for. I think it would have to be well defined up front, and I have nothing to add on the operational law.

COMMISSIONER WESSEL: No. My comment was this is simply a more in-depth conversation we need to have that there is no easy answer, and Dr. Mulvenon, I guess the question of enlightened implementation, there's been some questions of the enlightened implementation of the Patriot Act that some have had. So there are standards that have to be looked at very carefully.

DR. MULVENON: Commissioner, all I would tell you is that as a civil libertarian, I'm a robust user of personal encryption.

HEARING COCHAIR BROOKES: We'll end the panel on that note. Thank you very much for your testimony on this very important issue.

We'll adjourn for five minutes before we start the next panel.

[Whereupon, a short recess was taken.]

PANEL IV: ADMINISTRATION PERSPECTIVES

HEARING COCHAIR REINSCH: In our never-ending battle to keep on schedule, we're going to reconvene.

The next panel is not a panel; it's an individual. We are happy to welcome Ms. Patricia McNerney, who serves as Principal Deputy Assistant Secretary of State for International Security and Nonproliferation.

Her key responsibilities involve diplomatic efforts to address the proliferation challenges including Iran and North Korea; counterproliferation efforts to address the proliferation activities of states of proliferation concern and terrorists; implementation of multilateral treaties and initiatives and assistance programs; and support for civil nuclear programs consistent with nonproliferation principles.

Previously, she served as the Senior Advisor to the Under Secretary of State for Arms Control and International Security Affairs,

and served as the Republican Staff Director to the Senate Select Committee on Intelligence, and the Chief Counsel to the Senate Committee on Foreign Relations.

Thank you for being with us today. As per our rules, your full statement will be placed in the record, and we'd ask you to limit your oral remarks to seven minutes so that we have plenty of time for questions.

Thank you very much.

STATEMENT OF MS. PATRICIA McNERNEY, PRINCIPAL DEPUTY ASSISTANT SECRETARY OF STATE FOR INTERNATIONAL SECURITY AND NONPROLIFERATION WASHINGTON, D.C.

MS. McNERNEY: Thank you, Mr. Chairman, and thank you for the opportunity to appear before you today to discuss China's nonproliferation practices.

In my opening remarks, I'd like to point out a few areas where the U.S. and China have successfully cooperated on matters of nonproliferation, areas of some continuing concern, as well as some promising areas for new cooperation.

Let me say at the outset that the United States remains committed to working toward a relationship with China that enhances America's security, addresses China's legitimate concerns, and supports the security interests of our friends and allies.

We continue to engage China on nonproliferation matters in a constructive and forthright manner, building upon shared interests when possible, and raising concerns when necessary.

For its part, Beijing now recognizes that it has fundamental security interests in preventing the spread of weapons of mass destruction. It's now a party to the Nuclear Nonproliferation Treaty, the Biological and Toxin Weapons Convention, the Chemical Weapons Convention, is a member of the Nuclear Suppliers Group and the Zangger Committee.

China has been cooperative on efforts relating to North Korea and Iran. In the case of North Korea, China has made it clear that it does not condone Pyongyang's nuclear aspirations. They have joined the Security Council in unanimous votes to adopt sanctions resolutions, particularly 1718, following the North Korean nuclear tests, and they've continued to serve as the host of the Six Party Talks.

With regard to Iran, China shares our goal of preventing Tehran's acquisition of a nuclear weapons capability. Though differences of opinion remain on how best to achieve this end, China has joined with the other members of the Security Council in adopting Security

Council Resolutions 1713, 1747, and just recently 1803. As a member of the so-called P5+1, China has reiterated that should Iran continue to refuse to verification and compliance, additional sanctions will be necessary to augment those that are already in place.

Beyond this multilateral cooperation, China has expressed an interest and, in fact, taken actions with regard to export control cooperation including technical exchanges and training. To the extent that it's permissible within the law, we have endeavored to provide such assistance. For example, we have worked through our Export Control and Related Border Security Program to provide training to Chinese licensing and enforcement officials in areas such as practical inspection, targeting and investigation techniques.

Chinese nonproliferation policies have improved. However, a number of Chinese entities continue to supply to regimes of concern items and technologies useful in the weapons of mass destruction, their means of delivery and advanced conventional weapons. China continues to have important deficiencies in its export control system, particularly with regard to thorough implementation, transparent enforcement, and possibly willingness. We still observe Chinese firms and individuals transferring a wide variety of weapons-related material and technologies to customers around the world including Burma, Cuba, Iran, Sudan and Syria. We're particularly concerned that Chinese firms have continued to supply Iran with a range of conventional military goods and services in contravention of the restrictions of the Security Council resolutions. Evidence indicates that Iran has transferred weapons to Shia militants in Iraq as well as terrorists groups such as Hezbollah and the Taliban. For example, an Iranian version of the Chinese MANPADS system was used in Iraq in 2004. In addition, a Chinese QW-1, that we believe was provided by Iran, was recovered in Basra just this past April. We sanctioned a number of Chinese entities under the Iran and Syria Nonproliferation Act and pursuant to Executive Order 13382 for the sale of items on multilateral control lists or items with the potential to make a material contribution to ballistic or cruise missile programs or WMD programs.

China must devote additional resources to increased enforcement, rigorous implementation of catch-all provisions, and more investigations and prosecutions of violators of their laws. Moreover, China should share timely and substantive information on actions the government has taken in response to U.S. requests. We will continue as warranted to impose sanctions against Chinese entities engaged in proliferation and will continue to highlight our ongoing concerns about China's proliferation record with the government.

Sanctions, of course, always remain an option to deter proliferation behavior. We also need to develop effective inducements

that make clear it is in the best interests of China to enact and enforce rigorous nonproliferation policies. I'd like to discuss one particular initiative that my bureau has pursued.

There are a number of Chinese entities that after being sanctioned by the United States for proliferation related activity have seen their international reputations damaged and their exports dramatically reduced. Several sanctioned firms have expressed an interest in taking actions that would result in the relief from these sanctions.

This desire to come out from under sanctions gives us great leverage. As part of a broader nonproliferation strategy, we've held discussions with two major Chinese companies: the China North Industries Corporation, or NORINCO, and the China Great Wall Industries Company, both of whom have been sanctioned in the past for their proliferation-related activities. We've made absolutely clear to these entities that any trade in technologies useful in WMD programs or delivery systems would constitute proliferation-related behavior and would subject them to possible future sanctions. But we've also indicated that their decision to cease such proliferation activity would be recognized by the United States. A commitment to end proliferation-related activity would increase prospects that Western companies and international financial institutions would consider them to be legitimate corporate entities.

The response thus far has been very encouraging. The effort is, of course, only in its early stages. We need to ensure that these entities actually perform as they have pledged. However, the possible impact of success would be dramatic. To have NORINCO, a firm that has been sanctioned seven times since 2001, get out of the proliferation business would be a very positive development and one that could serve as an example to other Chinese companies.

In conclusion, the United States will continue to press China to implement effectively its export control regulations, eliminate loopholes in its laws, and reign in the proliferation activities of certain companies, and we'll continue to work with Chinese entities that have a serious desire to become corporate citizens of the international business community.

Continued proliferation by Chinese entities to countries of concern is neither in the U.S. interests nor in China's. Working together, however, we believe we can build upon a shared commitment to ensure an end to such proliferation activity.

Thank you.

[The statement follows:]

Prepared Statement of Ms. Patricia McNerney, Principal Deputy

Assistant Secretary of State For International Security and Nonproliferation, Washington, D.C.

Chairman Reinschmmissioner Brookes, Commissioners of the U.S.-China Economic and Security Review Commission, I'd like to express my appreciation for the opportunity to appear before you today and discuss China's nonproliferation practices. In my opening remarks I'd like to point out areas where the United States and China have successfully cooperated on matters of nonproliferation, areas of continuing concern, and some promising areas for new cooperation.

Let me say at the outset that the United States remains committed to working toward a relationship with China that enhances America's security, addresses China's legitimate concerns, and supports the security interests of our friends and allies. To that end, we continue to engage China on nonproliferation matters in a constructive and forthright manner – building upon shared interests when possible and raising concerns when necessary. We remain committed to expanding our areas of common interest with China, and improving our existing cooperation on nonproliferation. At the same time, we have serious concerns about the proliferation activities of certain Chinese entities and we continue, when necessary, to take action in response to those activities. We work constructively with China on a number of important proliferation issues, yet we also have made it clear that China must do more to halt the spread of WMD, missiles, and conventional weapons and related technologies.

Areas of Chinese Cooperation

The Government of China has come to recognize that it has a fundamental security interest in preventing the spread of weapons of mass destruction. In many ways, it has demonstrated its interest in becoming a responsible nonproliferation partner. It is now a party to many international nonproliferation instruments, including the Nuclear Nonproliferation Treaty (NPT), the Biological and Toxin Weapons Convention (BWC), the Chemical Weapons Convention (CWC), and is also a member of the Nuclear Suppliers Group (NSG) and the Zangger Committee. China has adopted export controls similar to the Australia Group control lists on chemical and biological related items, and has enacted missile-related export controls. And, the Government of China has approved a series of new laws and regulations designed to establish comprehensive national export control regulations.

China has cooperated in efforts to put pressure on Iran and North Korea via their role in the Six Party Talks. In the case of North Korea, China has made it clear that it does not condone Pyongyang's nuclear aspirations but admittedly has not actively cooperated to ensure closure of North Korean front companies inside China that facilitate proliferation or the Chinese companies that supply them. Following North Korea's missile launches of July 2006, and its October 2006 nuclear test, China joined in the Security Council's unanimous vote to adopt strong measures under UNSCR 1695 and UNSCR 1718, the latter of which imposed Chapter VII sanctions including a prohibition on transfers to North Korea of a broad range of conventional weapons, WMD-related items and luxury goods. China continues to serve as host to the Six-Party Talks, and has played a constructive role in formulating and implementing both the February 13, 2007 Initial Actions and the October 3, 2007 Second-Phase Actions agreements. With Chinese cooperation, the Six-Party process has brought us to the point where North Korea has agreed and begun to disable the three core facilities at Yongbyon -- the 5MW(e) Experimental Reactor, the Reprocessing Plant (Radiochemical Laboratory), and the Nuclear Fuel Rod Fabrication Facility. As we work to ensure that North Korea honors its commitments, continued Chinese support is pivotal in maintaining a united front.

With regard to Iran, China shares our goal of preventing Tehran's acquisition of a nuclear weapons capability. Though differences of opinion remain on how to best achieve this end, China has supported sanctions as a mechanism to increase pressure on Iran. China joined the other members of the Security Council in adopting UN Security Council Resolutions 1737 and 1747, and, just this March, UNSCR 1803.

These Security Council resolutions impose a series of Chapter VII sanctions on Iran. Among other things, these resolutions require Member States to prevent the supply to Iran of certain items, technology, training or financial assistance that could contribute to its proliferation-sensitive nuclear activities or its development of a nuclear weapon delivery system. The resolutions also require Member States to freeze the assets of entities and individuals who are identified in the UNSCR Annexes as having a significant role in Iran's nuclear and missile programs, and those acting on their behalf, or owned or controlled by them. Moreover, these resolutions prohibit Iran from exporting arms, urge Member States to restrict heavy arms transfers to Iran, and call for vigilance in the activities of financial institutions in their territories with all banks domiciled in Iran and their branches and subsidiaries abroad. Resolution 1803 calls on states to inspect certain cargo to and from Iran to prevent trafficking in the items prohibited under the relevant resolutions, and also targets those who have assisted designated entities and individuals in evading or violating UNSC sanctions. As a member of the P5+1, China has reiterated that, should Iran continue to refuse verification and compliance negotiations, additional sanctions will be necessary to augment those already in place.

These Chapter VII sanctions imposed on Iran and the DPRK send a clear and compelling signal that the international community will not tolerate the proliferation of weapons of mass destruction. And it is up to the entire international community to remain unified and consistent in its message to North Korea and Iran that international concerns regarding their nuclear and missile ambitions must be resolved.

Beyond our cooperation in multi-lateral venues that address proliferation, there are a number of instances where the Chinese have expressed an interest in export control cooperation, including technical exchanges and training. To the extent that it is permissible within the law, we have endeavored to provide such assistance.

One such example is the State Department's Export Control and Related Border Security (EXBS) Program, which has supported training for Chinese licensing and enforcement officials. Since 2006, the EXBS program has coordinated two training events to help Chinese Customs officers identify controlled commodities. These events were sponsored by the Department of Energy's International Nonproliferation Export Control Program (INECP) and took place in Shanghai and Dalian, focusing on training Chinese frontline Customs enforcement officials and technical experts responsible for interdicting illicit shipments of WMD-related, "dual-use," strategic commodities. EXBS also plans to offer Chinese Customs seaport interdiction training at the working seaport in Charleston, South Carolina.

Other interdiction-related activities include China's participation in the Department of Homeland Security's Container Security Initiative and the Department of Energy's Megaports Initiative. Both initiatives are aimed at improving detection of radiological and nuclear items at seaports.

In the area of industry-related export control-related training, EXBS sponsored a successful "Industry-Government Forum" for Chinese inter-ministry participation in mid-January, and plans to work with China on its development of an industry "Internal Control Program." Additionally, in coordination with the EXBS program, the INECP program is collaborating with the China Atomic Energy Authority (CAEA) within the CAEA-DOE Peaceful Uses of Nuclear Technology (PUNT) framework on the development of technical guides on nuclear and nuclear dual-use materials, equipment and technology. It is expected that these guides will enhance the capacity of Chinese licensing and industry specialist to evaluate export license applications and train Chinese industry and enforcement officials.

For the future, we expect China will agree to further exchanges on a wide variety of legal regulatory, industry outreach and enforcement issues, including practical inspection, targeting, and investigation techniques.

In addition to bilateral training initiatives, we also hope that China will join the Proliferation Security Initiative (PSI), which was created by President Bush to facilitate cooperation in the interdiction of nuclear, chemical and biological weapons, their delivery systems, and related technologies. The hallmark of the PSI is the close, innovative interaction between diplomatic, military, intelligence, law enforcement, and economic tools to combat proliferation. The PSI has become an important tool to interdict shipments, disrupt networks, and hold companies accountable for their activities. Beijing has thus far been reluctant to join with the almost 90 nations participating in the PSI, citing legal concerns. It also is quite possible that Beijing feels it must take regional concerns into account regarding its participation in the PSI, even though we have repeatedly clarified that PSI is not directed at any particular country. China's commitment and participation in the PSI effort would be in keeping with China's stated commitment to nonproliferation and would be a valuable contribution to international security. We will continue to address Beijing's concerns and emphasize that all PSI actions are taken in accordance with states' domestic authorities and international law.

Real Concerns Remain

The proliferation policies of the Government of China have improved. However, a number of Chinese entities continue to supply items and technologies useful in weapons of mass destruction, their means of delivery, and advanced conventional weapons to regimes of concern. We continue to find that China has important deficiencies in translating its declared nonproliferation objectives into its export control system, particularly with regard to thorough implementation, transparent enforcement and possibly, willingness.

We continue to engage the Chinese government in an effort to halt commercial transactions that violate UNSC Chapter VII sanctions, nonproliferation norms, and Chinese law, but our efforts are met with mixed results. We still observe Chinese firms and individuals transferring a wide variety of weapons-related materials and technologies to customers around the world that we judge would use or retransfer the weapons in a manner that threatens regional stability and international security – including to Burma, Cuba, Iran, Sudan and Syria.

In addition, we have raised with the Chinese government our concerns that Chinese seaport facilities and international airports are transit and transshipment points for governments and entities that wish to ship sensitive materials to programs of proliferation concern. Certainly we would hope that China wishes to avoid a global reputation as a safe transit and transshipment point for foreign proliferators.

Judging the extent to which the Chinese government or Chinese officials are witting of the proliferation activity of Chinese entities is difficult given the lack of transparency noted earlier. One factor enabling proliferation activities is the decentralization that has become a key feature of China's economic reform. We simply do not know enough about China's export control regime, and cannot assess the level of control or awareness that Chinese officials have over increasingly free-wheeling companies that trade in dual-use materials applicable to WMD and their delivery systems. These transfers remain a serious concern, and we will continue to press Chinese officials to be vigilant and act vigorously to investigate and enforce their export control regulations.

We are particularly concerned that Chinese firms have continued to supply Iran with a range of conventional military goods and services in contravention of the restrictions within these UN Security Council Resolutions. Inevitably, some of this weaponry has found its way to insurgents and militants operating in Iraq, as well as Hizballah terrorists in the Levant. The United States has sanctioned a number of Chinese entities under the Iran and Syria Nonproliferation Act and Executive Order 13382 for the sale of items on multilateral control lists or items with the potential to make a material contribution to ballistic or cruise missile programs or WMD programs.

With specific reference to conventional weapons, China, like many other countries, views its trade in conventional weapons as helping nations to meet their perceived defense needs and asserts that these transfers are in accordance with international norms. Despite this assertion, evidence indicates that Iran has transferred Chinese weapons to Shia militants in Iraq as well as terrorist groups such as Hizballah. For example, the Misagh-1 (the Iranian version of a Chinese MANPADS with Chinese components) was used in Iraq in 2004. In 2006, a Chinese C-802 anti-ship cruise missile, which has been supplied only to Iran in the region, was used by Hizballah to attack an Israeli naval vessel. China appears to accept at face value the end-use assurances and pledges against retransfers it receives from its customers, despite the fact that some of its customers have links to terrorists and have records as unreliable end-users, such as Iran. Nevertheless, China has demonstrated sensitivity to growing international concerns about recipients of some of its arms sales, notably Sudan. We continue to seek greater Chinese cooperation in curtailing transfers to state sponsors of terrorism and in stricter and more uniform application of its export control safeguards.

We have discussed with China the importance of addressing its weak export control enforcement and detection capabilities in order to rein in the proliferation activities of certain Chinese companies. If China is to have in place a rigorous export control system, it must devote additional resources, increased enforcement, rigorous implementation of catch-all provisions, and more investigations and prosecutions of violators of its export control laws. Moreover, we have encouraged China to share timely and substantive information on actions the government has taken in response to U.S. demarches. A level of transparency in China's nonproliferation activity is absolutely essential; heretofore this has been notably lacking. We will continue, as warranted, to impose sanctions against Chinese entities engaged in proliferation and will continue to highlight our ongoing concerns about China's proliferation record with the Chinese government.

An area of potential concern is possible additional Chinese support for Pakistan's civil nuclear program. As a member of both the NPT and the NSG, China has shown its commitment to enforcing international nonproliferation and export control norms. When China joined the NSG in 2004, it made a statement regarding the safeguarded nuclear facilities in Pakistan it would continue to support as "grandfathered." These are: the Karachi nuclear power plant; Chasma nuclear power plants 1 and 2; and Parr research reactors 1 and 2. Recently, Pakistan has expressed interest in increasing domestic nuclear power generation and has made overtures to China for support. This is something we continue to watch closely to ensure both that China abides by its commitments to the NSG and to ensure that ongoing Chinese cooperation with Pakistan does not support Pakistan's un-safeguarded nuclear weapons program.

Areas of Promising New Cooperation

Sanctions, of course, always remain an option to deter proliferating behavior. We have made an effort to use these sanctions in a targeted and constructive way. Avoiding those sanctions is a strong inducement for legitimate Chinese corporations to enact and enforce rigorous nonproliferation policies. As an alternative to sanctions, we have worked to encourage China to become a willing partner in addressing a common nonproliferation agenda.

Mr. Chairman, to this end, I would like to discuss one particular initiative that my bureau has pursued. As I have already noted, there are a number of Chinese entities who, after being sanctioned by the U.S. for proliferation related activity, have seen their international reputations damaged and their exports dramatically reduced. Several Chinese firms sanctioned under U.S. law or Executive Order have expressed an interest in taking actions that would result in relief from the sanctions. We can leverage this desire by Chinese firms to come out from under sanctions and advertise the tangible benefits that can accrue to companies that wish to abandon proliferation.

As part of a broader nonproliferation strategy that we devised last year, we held discussions with two major Chinese companies – the China North Industries Corporation (NORINCO) and the China Great Wall

Industries Company (CGWIC) – both of whom have been sanctioned repeatedly in the past for proliferation-related activities. We have made absolutely clear to these entities that any trade in technologies useful in WMD programs or delivery systems would constitute proliferation-related behavior, and would subject them to possible future sanctions. We also continue to make it clear to them that any conventional arms transfers to countries such as North Korea and Iran are equally unacceptable. But, we have indicated that their decision to cease such proliferation activity would be recognized by the United States. A commitment to end their proliferation-related activity and concrete, positive action towards this end would likewise increase prospects that Western companies and international financial institutions would have no concerns in developing broad economic and trade ties with these Chinese companies.

The response of NORINCO and CGWIC has been very encouraging. Both companies have adopted comprehensive internal compliance programs and are implementing policies to ensure that inadvertent transactions do not occur. NORINCO, for example, has committed to refrain from selling armaments to North Korea or Iran and claims to have turned down over $100 million in potential contracts with sanctioned regimes. And there are indications that the positive results are not limited only to these two companies. I fully anticipate that if tangible benefits of a solid nonproliferation record begin to accrue, additional Chinese companies will seek to emulate the nonproliferation policies of NORINCO and CGWIC.

This effort is, of course, only in its early stages. We need to ensure that these entities actually perform as they have pledged. We need to make sure they do not simply spin-off their proliferation-related activity to subsidiaries or sister companies so that the problem remains under another guise. And, these companies need to demonstrate that they are committed to the path of good corporate citizenship over the long haul. However, the possible impact of success would be dramatic. To have a commitment from a company such as NORINCO, a firm that has been sanctioned seven times since 2001, to get out of the proliferation business is a very positive development and one that could serve as an example to other Chinese companies. I am guardedly optimistic that our efforts can bring about meaningful results.

Conclusion

The United States will continue to press China to implement effectively its export control regulations, eliminate loopholes, and reign in the proliferation activities of certain companies. And we will continue to work with Chinese entities that have a serious desire to become good corporate citizens of the international business community. Continued proliferation by Chinese entities to countries of concern is neither in U.S. interests, nor China's. Working together, we can build upon our shared commitment to ensure an end to such proliferation activity.

Panel IV: Discussion, Questions and Answers

HEARING COCHAIR REINSCH: Thank you.

Commissioner Videnieks.

COMMISSIONER VIDENIEKS: What is the scope or how do we define proliferation now? I just heard you mention advanced conventional weapons as being included. It used to be just WMD and CBR maybe. So that's the question basically. What is the scope and when did advanced conventional weapons-- and what are they--get added, and how about the AK-47s?

MS. McNERNEY: Yes. Obviously, we've always obviously been

concerned about chemical, biological and nuclear ballistic missile systems, but the Iran, Syria, Nonproliferation Act, now the Iran, North Korea, Syria Nonproliferation Act added conventional weapons as an area that we have to review for sanctions activity. As a result of that act of Congress, Chinese companies that are supplying conventional weapons to Iran are subject to sanctions under U.S. law.

COMMISSIONER VIDENIEKS: How about the foreign military sales? How does that fit into--I mean a sale is a method of proliferation. It's a tool.

MS. McNERNEY: Sure. Yes.

COMMISSIONER VIDENIEKS: I guess the recipient is the one that determines whether it's negative or positive; right?

MS. McNERNEY: Yes. For example, take NORINCO. They have long-standing contracts with Iran for conventional weapons. That has been an area that we have tried to encourage China to get out of the business of selling weapons, even conventional weapons, to Iran, to Syria, to North Korea, because of the destabilizing influence of those weapons. And even when NORINCO does sell the weapons, they are consistent with what they perceive as their laws and responsibilities. We find they take for granted when Iran assures them that the end-user is, indeed, Iran and that the weapons are for defensive capabilities. Yet we find them in Iraq on the battlefield. We find them with Hezbollah. So the proposition that Iran is a responsible actor, or the argument that conventional arms sales to Iran would be considered traditional defensive capabilities, just doesn't play out when you look at the facts on the ground.

COMMISSIONER VIDENIEKS: Thank you.

HEARING COCHAIR REINSCH: Commissioner Wessel.

COMMISSIONER WESSEL: Thank you for being here. Two, I think, relatively quick questions.

You mentioned shipments to Cuba, that those had been discussed with China. Can you let us know what the nature of those shipments were because you mentioned advanced weaponry and the other categories?

MS. McNERNEY: Maybe I can get back to you sort of what specifically we've seen. I don't think we've seen anything beyond, you know, sort of standard conventional arms that have gone to Cuba. Certainly we wouldn't put that in the WMD or ballistic missile category.

COMMISSIONER WESSEL: Okay. If you could get back to us on that, that would be appreciated.

MS. McNERNEY: We'll get that to you.

COMMISSIONER WESSEL: Also, as we look at the broad infrastructure laws, are you also engaged in Export Control Act post-

verification reviews? Is your office aware of that? And what has been the Chinese implementation of the post-verification review process in the last year or two?

MS. McNERNEY: Yes. We do a little bit less of that. We refer to our Political Military Bureau for implementing the military side of post-shipment verification, but we do obviously work with the Commerce Department and the other parts of the State Department to look at which entities are actually following through on the export requirements.

For example, if we sell a military-related item that could be used for dual-use purposes, and those companies then are retransferring them to countries of concern, we'd obviously look at it for sanctions possibilities as well as simply to try to stop the retransfer activity. We would talk to the Chinese government about the activity. But my bureau wouldn't get in the business of the sort of regulatory aspects of U.S. export law.

COMMISSIONER WESSEL: Understand. But as it relates to verification, the actual visits in China which could, as you pointed out-

MS. McNERNEY: Yes.

COMMISSIONER WESSEL: --result in transshipment and potential problems or misuse in the dual-use area, has China changed its practices or are they allowing more verification visits? Has that accelerated? What's been the experience in the last couple of years?

MS. McNERNEY: Some countries are more forward leaning than China about opening up their books. I think you'd have to talk to our Commerce Department folks who actually initiate the visits, but I think it's not always as open as we would like with all Chinese entities. So probably a mixed bag.

COMMISSIONER WESSEL: Okay. Thank you.

HEARING COCHAIR REINSCH: Commissioner Fiedler.

COMMISSIONER FIEDLER: I'd like to pick up on your NORINCO discussion. So NORINCO gets sanctioned seven times and now says it's a good actor and cooperates with training and other things with us in the United States I think at the University of Georgia or somewhere.

Is their former activity simply being picked up by Polytechnologies or some other bad actor in China? So whereas NORINCO has gotten out of the business, has some other entity gotten in and we don't see a diminution?

MS. McNERNEY: Yes. That's one of the things that I worry about when we're looking at engaging a Chinese company. I think on one level, you want NORINCO obviously to clean its act up and we need to do everything we can to give it sort of that gold star. But it's

not simply them telling us what they're doing--

COMMISSIONER FIEDLER: Oh, no, I understand.

MS. McNERNEY: --but actually seeing the experience. But that said, because of the structure of Chinese state-owned corporations, you can simply move the sanctionable activity to an entity you don't care about getting sanctioned and therefore be able to continue the business and avoid the sanctions. That's something that we've really focused in on. It's not only cleaning up the entities but also changing the Chinese policies and sort of mind-set about who are valid customers for some of these military-related goods. For example, we don't think any Chinese entity should be selling conventional arms to Iran at this time. That's certainly our strong message to China on the policy front. We're trying to also get the companies involved.

One of the things that NORINCO has been doing which is impressive is setting up an Internal Compliance Program, like any other multilateral or multinational company would do in the United States, Europe, or any other normal Western-like companies. We think that's a really important move. If it starts to become a way of operating, a business model for Chinese companies down the line, I think that's all to the good and certainly improves these larger companies as actors.

But there still is that issue obviously of the Chinese policy and what they see as a legitimate and valid sale. That, I think, is what you're getting at, which is that we don't want a shell game where they just kind of move it over to another company.

COMMISSIONER FIEDLER: Have we seen a diminution in their conventional arms trading with Iran?

MS. McNERNEY: We have, and I think it's fair to say the Chinese, too, find the image they want to portray to the world an image that they are not selling arms that are killing American soldiers in Iraq. So there is sensitivity on their part to making sure their companies are not engaged in activities that are ending up in retransfers from Iran.

I think time will tell whether this is something they are simply doing in advance of the Olympics in order to embarrassment during such a high profile activity. We're going to want to see this activity beyond then and see if it's going to hold more permanently.

COMMISSIONER FIEDLER: Thank you.

HEARING COCHAIR REINSCH: Commissioner Mulloy.

COMMISSIONER MULLOY: Thank you, Mr. Chairman. Thank you for being here, Ms. McNerney.

On page four of your testimony, you tell us that we continue to engage the Chinese government in an effort to halt commercial transactions that violate UNSC, meaning U.N. Security Council,

Chapter VII sanctions.

Are these sanctions that we have put on Iran to try and head off Iran from pursuing the development of nuclear weapons?

MS. McNERNEY: Yes.

COMMISSIONER MULLOY: Yes. Then, later you say we are particularly concerned--so the Chinese must have voted in favor of those sanctions?

MS. McNERNEY: Yes. I want to be careful that we're talking about Chinese entities and not the Chinese government that are engaged in that activity. There are a number of Chinese entities that we think are still engaged in sale of dual-use technologies that might end up, for example, in the nuclear program. The Chinese I think from a legal standpoint would say: "Look, we've got the laws in place, we're going to enforce this, but we're still seeing some of those entities evading those rules and enforcement mechanisms."

COMMISSIONER MULLOY: Did the sanction adopted by the Security Council, and the Chinese must have voted for it if it was adopted, or at least--

MS. McNERNEY: They did, yes.

COMMISSIONER MULLOY: Yes. Did that cover conventional weapon sales to Iran?

MS. McNERNEY: On the conventional side, the Security Council Resolutions ask countries to be very wary of any sales in the conventional side, and to I think it's "vigilance and restraint" or some terminology like that. And we certainly have pressed countries, including Russia as well, that vigilance and restraint given the facts on the ground, particularly in light of transshipments or transfers to terrorist organizations, means that they shouldn't sell anything. But the resolutions do not say that.

COMMISSIONER MULLOY: Do they disagree that this is covered by the Security Council Resolution?

MS. McNERNEY: They believe that they are acting with appropriate restraint and vigilance, yes.

COMMISSIONER MULLOY: Okay. Then one other question. You mentioned the Proliferation Security Initiative, and you mentioned that the Chinese have been reluctant to join the other 90 nations that are part of that, and you say that they cite legal concerns. What are those legal concerns?

MS. McNERNEY: The Proliferation Security Initiative statement of principles says that we're going to take all actions consistent with national legal authorities and international law. In the five years now that the PSI has existed, we really have acted in that manner. The Chinese still are concerned that we're going to use it to justify at-sea boardings that are outside of international legal

requirements and that sort of work.

COMMISSIONER MULLOY: Boarding ships?

MS. McNERNEY: Yes. Certainly there are obviously legal requirements if one were to actually board a ship on the high seas. There's a Chinese concern that PSI would be seen as a green light for broader enforcement actions than are currently required under international law.

COMMISSIONER MULLOY: I see. Thank you very much.

HEARING COCHAIR REINSCH: Commissioner Esper.

COMMISSIONER ESPER: Thank you, Ms. McNerney, for being here this afternoon.

I got a couple questions. First of all, I'm trying to connect the dots between what we discussed in this morning's panels, and that involved space issues and space technologies, and your testimony. Within the portfolio of your division, your bureau, do you see any Chinese shipment or the receipt of space-related items or components that may help the PRC advance its space capabilities? Are you seeing any type of trade such as that?

MS. McNERNEY: You know, I think in previous times there was a little more of I think some violations of our own export control laws, but I don't think there have been any high profile cases of that nature in the last several years.

For China Great Wall, commercial space satellite launch service is their business. They are under sanctions. They'd very much like to get out from under that sanctioning so that they can engage in legitimate civilian launch activities, and so--

COMMISSIONER ESPER: They're under U.S. sanction?

MS. McNERNEY: They're under our Executive Order 13382 dealing with proliferation finance. That's been a real impediment as they do business around the world. Banks don't want to do business with companies on those lists. So there's real incentive for them to get back into the business. That's part of the reason there's a lot of effort to clean up their proliferation practices.

Yes, our own export control law enforcement measures are not an area that my bureau tracks as much so I wouldn't have as much familiarity.

COMMISSIONER ESPER: Right. The other part of this morning's hearing was focused on trying to figure out what China is doing in the domains of space and cyberspace, what their grand strategy is, and what their ambitions and aims are.

From your perspective, with regard to proliferation, what conclusions do you draw? Are they honestly trying to control entities that are proliferating or do you think their actions are part of a broader strategy? Has your bureau drawn any conclusions about what you may

be seeing?

MS. McNERNEY: Where we've looked at this in more detail is the recent anti-satellite test that they did about a year-and-a-half ago. We saw that as very problematic. They didn't notify anyone prior to the test, there was no transparency, the debris that is up there could be there for over a hundred years, and that could have impact on civilian assets in space. We've pressed them very hard on that side of it.

Meanwhile, they've pressed for a treaty in the Conference on Disarmament context that we think actually doesn't address some of the real issues that we're dealing with in terms of the anti-satellite testing and so forth. The Chinese space arms control proposal looks to control and pull back some of our own broader space activities. So, that's one area where obviously they're looking to accelerate their own technical capabilities in space, but try to do so in a way that hems in some of the activities that others are engaged in.

Any kind of sales to Iran, for example, which is interested in space-based capabilities, would be a violation of the Security Council Resolutions. That's an area where some Chinese companies might be engaged in exporting some of the materials. So that would be another focus for activity.

But space obviously is an area where there's a lot of interest and movement, and you know I'm sure that our Political Military Affairs Bureau colleagues or our Commerce colleagues can talk more about what China is doing in the United States to gain some of that capability here.

COMMISSIONER ESPER: What's your overall scorecard though, for China on proliferation? We've discussed this now over at least a decade. Is it better than it was and getting better and therefore it reflects their desire to be a responsible stakeholder, as the saying goes? Or do you see it as unchanged and unclear why it's not changing or improving?

MS. McNERNEY: I think it's better. I think they are definitely making progress legally across the board. They've got laws in place now. Even on specific areas, when they really want to send down an edict to stop a certain kind of shipment, somehow that activity does dry up a bit.

We've had a lot of success where these Chinese companies and banks want to get into international financial markets, where they want to play on a field that allows them the access. So Chinese financial institutions are probably more aggressive in terms of not engaging with sanctioned entities that could then cut them off financially from Europe or from the United States.

The companies themselves, as I mentioned, have a similar sort of a similar calculus. At the same time, there are a lot of these smaller

actors that seem to just continue with the proliferation activities and seem to get away with it. We'd like to see more effort focused on the enforcement side because there seems to be the ability of these kinds of companies that want to act outside Chinese export control law to get their goods to market. That's really where we've focused a lot of our energy and attention.

COMMISSIONER ESPER: Okay. Good. Thank you.

HEARING COCHAIR REINSCH: Thank you. Commissioner Shea.

COMMISSIONER SHEA: Thank you very much for being here this afternoon. Just two quick questions. First of all, would you like to have any additional tools or authorities so that you could do your job at curbing proliferation of weapons, so they can do it more effectively? That's my first question.

And secondly, we recently saw China trying--I guess it's a Chinese company--Polytechnologies--trying to ship conventional arms to Zimbabwe. I believe that shipment was stopped in South Africa by--

MS. McNERNEY: It's actually in Angola.

COMMISSIONER SHEA: Angola. Thank you. Do you--and then sent back home--do you see any reassessment among the Chinese leadership that maybe these types of activities are not good for the brand? That maybe, you know, in the short run or in the long run or even the short run, this is not a useful activity to be engaged in, not beneficial for China's image?

MS. McNERNEY: Yes. Just on the first question regarding the tools. I do think we have pretty broad sanctions authorities if we need them, with the Executive Orders that target financing. That's been a really valuable tool since the President issued that order.

A lot of it is political will and dialogue, and highlighting the issue and just continuing to press away. Frankly I think the Chinese government acts more when these things are highlighted in a public way and they see the down sides such as those that you mentioned about the shipment.

The arms shipment to Zimbabwe would have gone had it not been for this international scrutiny and attention. So I think all of this kind of discussion really is valuable in terms of augmenting the legal tools. I don't think there's some tool missing that we're hoping for.

Regarding that second point, we have seen some decrease. What we're concerned is that improvements in Chinese nonproliferation practices are because of public attention that is the result of a little more attention on the Olympics and anything that's high profile nature. But, they have pulled back some from Iran. They don't sell as much to North Korea or allow their companies to sell spare parts, that sort of

thing.

At the same time, you know, I think they come under tremendous pressure from their businesses to create jobs and get sales out the door and increase exports, just like most governments would. That really requires some strong positions from the government to sort of push back on those kinds of sales. It's a challenge. They perceive that legitimate defensive weapons are not sanctionable or not prohibited under their laws and, therefore, we're acting extra-legally by applying these sanctions. Obviously, we disagree. We think it's important to take a stand when you talk about selling arms to such regimes. But it is an area that we tend to differ.

COMMISSIONER SHEA: Thank you.

HEARING COCHAIR REINSCH: I have a couple of questions and then we'll have a second round. We have at least one commissioner who has an additional question.

With respect to the conventional arms transfers that you alluded to, Cuba, wherever, I understand those are things that we wouldn't want them to do as a matter of policy. Are those also violations of multilateral obligations the Chinese have undertaken?

MS. McNERNEY: No, I think I'd put it in the category I just mentioned, that our own sanctions laws would look at transfers to states that we list as state sponsors of concern, the terrorist list designated countries. Where we put our focus and energy frankly is Iran, North Korea, Syria -- countries where we truly see a security threat. Then there are others who would focus a little more on some of the countries with humanitarian concerns, like a Sudan or Zimbabwe.

So I think that's probably where the focus of efforts and energy in terms of talking to the Chinese about these sales would go.

HEARING COCHAIR REINSCH: Okay. I was trying to draw the distinction between situations where they violate obligations they've undertaken and situations where they're simply doing something we don't like.

MS. McNERNEY: Yes. I mean I think that's how they would present it to us, that they're not violating any international legal requirement. I think they would say that we're acting extralegally by imposing sanctions on such transfers. We have to look at this from our context of our own laws and responsibilities.

HEARING COCHAIR REINSCH: Would you support trying to bring them into the Wassenaar Arrangement?

MS. McNERNEY: I'll have to double-check whether they're in Wassenaar or not.

HEARING COCHAIR REINSCH: No.

MS. McNERNEY: They are not in Wassenaar. They are obviously in the NSG at this point, but one of the things to —gain

membership is obviously the ability to meet certain standards. Until they're ready to meet those standards, there is unlikely to be consensus to get into any of the arrangements.

MTCR is another one where there's an interest for them to join, but we believe that they, or some of their companies, are still selling missiles. Their companies are selling items that are going into, for example, Iran's or Syria's ballistic missile programs, and so forth. So until we get these entities really acting in a way that meets what we would see as the legal baseline, then I think we'd be unwilling in the Wassenaar or MTCR context to be supportive.

HEARING COCHAIR REINSCH: You just said one of the magic words, which is their companies are selling. The issue that comes up every time we have this discussion is the extent to which the transfers, for lack of a better term, are at the direction of or knowledge of the Chinese government or whether they are entrepreneurial, if that's the right word, by people trying to make money or trying to achieve other objectives.

Do you have a view on the extent to which it is one or the other?

MS. McNERNEY: I think Chinese government on WMD and ballistic missile kinds of transfers has a pretty firm policy not to be supporting the proliferation of those programs, but it's a number of these entities that are engaged in this business.

Where we press the Chinese is the enforcement or the follow-up side. That's where it's sometimes a challenge for the Chinese entities to take our word for it that we think the end-user is a bad actor and not just a legitimate kind of business engaged in something that wouldn't be seen as a violation of the Security Council resolutions.

A lot of times the Iranian entities, for example, will mask who they are when they approach these Chinese companies. Iranian entities will present different front names and will look like a legitimate transaction. But some Chinese companies continue to engage in prohibited sales with Iranian front companies even after being made aware of some of this information. That's when you know it's a willful ignorance in terms of what the end use is.

HEARING COCHAIR REINSCH: And do you find situations in that category where the Chinese government ends up cooperating and taking some action against its own, its company or entity?

MS. McNERNEY: Yes, I think sometimes their approach is less of enforcement the way we would expect when there's a U.S. company that violates these laws. In the United States we've got real enforcement actions and tools. There's a sense I think on the Chinese side that that would sometimes bring embarrassment. They try to deal with it maybe more quietly talking to the company, trying to change their mechanism, their ways. It's a different approach, and obviously

we've encouraged them to be a little more forceful on the enforcement side of their laws.

HEARING COCHAIR REINSCH: Yes. Thank you for that.

Commissioner Fiedler.

COMMISSIONER FIEDLER: You mentioned briefly in your testimony about the Port Security Initiative. Could you give us a quick update--we got into it a little bit last year--in a statistical sort of way, not the number of ports that they are cooperating with us on, but what that represents as the percentage of container traffic, which is probably the more meaningful number?

MS. McNERNEY: Yes, I think I talked about the Proliferation Security Initiative in my testimony.

COMMISSIONER FIEDLER: Well, any--

MS. McNERNEY: Other agencies of the U.S. Government really run those programs so I can get you those statistics. I wouldn't have them off the cuff.

COMMISSIONER FIEDLER: Okay.

MS. McNERNEY: Yes.

COMMISSIONER FIEDLER: All right. Thank you.

HEARING COCHAIR REINSCH: I think we have just time for one question each if that's all right. Commissioner Mulloy first and then Commissioner Esper.

COMMISSIONER MULLOY: Ms. McNerney, I did want to thank you for your many years of distinguished service to the Republic in a lot of different public policy positions.

In the conventional weapons, Commissioner Videnieks and I were just talking about that. The United States, I believe, is the largest conventional arms seller in the world.

MS. McNERNEY: That's right.

COMMISSIONER MULLOY: Is that your understanding?

MS. McNERNEY: I think that's probably accurate.

COMMISSIONER MULLOY: Now, are there multilateral agreed restrictions on the sale of conventional arms?

MS. McNERNEY: There is the Wassenaar Arrangement which sets out the conditions multilaterally by which we as a nation along with other Wassenaar partners have agreed to make such sales so we obviously try to meet all those multilateral requirements we've agreed for ourselves. The U.N. also has conventional lists in arms obviously that require greater scrutiny and greater detail. As for countries that are under U.N. sanctions, it does seem odd to be engaged in arms activities with those countries while they're under U.N. Security Council sanctions.

COMMISSIONER MULLOY: Okay. Thank you very much.

HEARING COCHAIR REINSCH: Commissioner Esper.

COMMISSIONER ESPER: On your point with regard to enforcement and implementation that you answered for me and Commissioner Fiedler, do you have any sense of how many people or how large the bureaus are in China for export control enforcement and implementation?

MS. McNERNEY: Why don't I get you those numbers? It's a different agency outside the Foreign Ministry that would handle that obviously.

COMMISSIONER ESPER: Right.

MS. McNERNEY: Let us look at those.

COMMISSIONER ESPER: Okay. I just ask the question to also suggest that I think it's significantly lower than the 30,000 or 40,000 that are reportedly monitoring the Internet and would question, therefore, whether it's a matter of priority for Beijing to ensure implementation and enforcement of their export control policies, laws and regulations.. So, for the record, I throw that out there. Maybe we can discuss it some other time.

HEARING COCHAIR REINSCH: I think we can safely say it's a smaller number than their number of people working on the Internet.

Thank you very much, Ms. McNerney, for your time. We appreciate it and we appreciate your staying with us.

We'll move now to the next panel if they'll come forward.

PANEL V: CHINA'S PROLIFERATION PRACTICES

HEARING COCHAIR REINSCH: All right. If the witnesses will take their seats, we'll get started, and it's my pleasure to introduce them for our last panel which will examine China's proliferation practices and nonproliferation commitments and policies.

Our first witness is the Honorable Stephen Rademaker, who is currently Senior Counsel at BGR Holding, LLC, here in Washington.

From 2002 to 2006, he served as Assistant Secretary of State heading at various times three bureaus including the Bureau of Arms Control and the Bureau of International Security and Nonproliferation. He directed nonproliferation policy toward Iran and North Korea as well as the Proliferation Security Initiative.

Not sure you'd want to put all of that in your resume, but there it is. He also had an extensive career with the House of Representatives Foreign Affairs Committee, as I recall.

Henry Sokolski is the Executive Director of the Nonproliferation Policy Education Center, a Washington-based nonprofit organization founded in 1994, to promote a better understanding of strategic weapons proliferation issues for academics, policymakers and the media.

He served from 1989 to 1993 as Deputy for Nonproliferation Policy in the Office of the Secretary of Defense and received the Secretary of Defense's Medal for Outstanding Public Service.

I would say it's nice to see you Henry. We have not often agreed over the years, but I always learn something when I listen to you, and I'm looking forward to learning something again today.

Thank you both for testifying. As with the last panel, we'll put your full statements in the record. You have seven minutes each and then we'll have time from the looks of things several rounds of questions, and we'll begin with Mr. Rademaker.

STATEMENT OF THE HONORABLE STEPHEN G. RADEMAKER
SENIOR COUNSEL, BGR HOLDING, LLC
WASHINGTON, D.C.

MR. RADEMAKER: Thank you, Cochairman Reinsch. I see that Cochairman Brookes does not appear to be here. He's a former colleague of mine.

HEARING COCHAIR REINSCH: Don't take it personally.

MR. RADEMAKER: I will not.

HEARING COCHAIR REINSCH: He's traveling and had to leave a little early.

MR. RADEMAKER: Understood. I appeared before this Commission in 2005. At that time, I was actually in the position that Patricia McNerney is now in, and so I spoke to you as an administration witness.

HEARING COCHAIR REINSCH: And yet we invited you back.

MR. RADEMAKER: Yes.

HEARING COCHAIR REINSCH: Congratulations.

MR. RADEMAKER: Don't know what possessed you. I now speak only on behalf of myself. That means I'm free to say whatever I actually think as opposed to what the interagency consensus is about the matters before this Commission.

COMMISSIONER FIEDLER: You're free to add to your previous testimony.

MR. RADEMAKER: Well, it's been a few years so I don't really recall what I said three years ago, but I would say the disadvantage of appearing on your own behalf is that you don't have a staff to prepare your remarks for you, so you get to say what you want to say, but it proves to be much more time consuming to think through what you want to say.

I've prepared a written statement which I have submitted. I will do you the courtesy of not reading it to you. You may read it at your leisure, but I will simply summarize some of my main points now.

I noted at the outset of my testimony that I'm not currently reading intelligence about China's proliferation practices so I'm not in a position to give you an up-to-date assessment of what China is doing today.

I thought what I could most usefully do is talk a little bit about my experience as a U.S. government official with responsibility for talking to the Chinese government about proliferation problems, and give you a feel for what that was like, and share with you some of my observations and conclusions on the basis of that experience.

One of the main points I make in my testimony is that as a U.S. government official charged with talking to the Chinese government about nonproliferation issues, I talked to my counterparts, and almost without exception my counterparts were out of the Chinese Foreign Ministry, and I found them to be good, serious, interlocutors who I came to believe over time really wanted to do the right thing in the area of nonproliferation. I had every reason to believe that they shared the philosophy underlying nonproliferation.

But over time I also came to the view that they were not the ultimate authority within the Chinese government, and particularly with some of the problem cases that we dealt with repeatedly in our discussions with them, my conclusion ultimately was that they simply did not have the authority within their system to address the problem. What exactly the nature of the problem was within the Chinese government I'm not in a position to be able to say with certainty, but I think the results speak for themselves. There were cases, and we called them the serial proliferators, where we essentially ran into a brick wall.

So the only policy resort that we within the U.S. government had in such cases was to resort to the imposition of sanctions pursuant to U.S. law or U.S. executive order. Chinese government officials would always become upset at that. They would see that as an affront, as unilateralism. We talk less today about American unilateralism than we did a few years ago, but the Chinese would often use that term with us.

I was deeply gratified to read in Secretary McNerney's testimony about two of the companies that we regarded as serial proliferators during my time at the State Department and how they have apparently of their own accord entered into dialogues with the U.S. government about how to avoid being sanctioned going forward. To my mind, that is perhaps the best advertisement I've ever seen for the U.S. policy of imposing sanctions on foreign entities that engage in unacceptable proliferation practices.

The philosophy underlying the imposition of sanctions and our sanctions laws is not, as I point out in my testimony, to actually impose sanctions; it is to change behavior. And in that sense, any time

we have to actually impose sanctions, that's fundamentally a failure of our policy because again our policy is not to impose the sanctions; it's to give rise to a world in which it's unnecessary to impose sanctions because companies are behaving.

The fact that two of the serial proliferators are now talking to the United States government about how to behave better in the future is exactly the kind of conduct that these laws are intended to promote, and so I read that with great satisfaction. I can recall in the wake of the enactment of some of these laws, and I was a congressional staffer at the time and had some hand in helping craft these laws, there was a debate about the efficacy of sanctions: does this approach make sense?

And there were voices that said no, it does not make sense. I think Secretary McNerney's testimony stands for the proposition that, in fact, you can see results as a consequence of U.S. sanctions laws.

One other issue that I address in my testimony is that of financial sanctions. I would call this a new frontier in U.S. sanctions policy. It's a frontier that really was opened during the Bush administration. There was the executive order on WMD financing, Executive Order 13382, which issued in 2005, as well as a near simultaneous action under Section 311 of the U.S.A. Patriot Act to declare Banco Delta Asia a primary money laundering concern because of its involvement in illicit transactions involving the North Korean government.

I can tell you as someone who was in the U.S. government at the time that these two initiatives were undertaken that they really got the attention of the Chinese government. The Chinese government did not know what to make of the actions of the U.S. government, but I think it perceived that they potentially could inflict real economic pain, perhaps not on the Chinese economy writ large, but on an additional sector of the Chinese economy that in the past had not felt any exposure or any risk of exposure because of misconduct in the area of proliferation, and that was the financial sector of the Chinese economy.

I describe in my testimony how in the next regularly scheduled consultation between the U.S. government and the Chinese government following the adoption of these two measures, for the first time ever, our Chinese counterparts from the Foreign Ministry arrived in the company of Chinese banking officials who had lots of questions about what it was we were up to. What standards were we applying? What was it that they had to do to avoid finding themselves in the position of Banco Delta Asia? What criteria would be applied in the freezing of assets?

With the assistance of officials of the U.S. Department of

Treasury, we very patiently described to them what the U.S. policy was about, how the executive order worked, how Section 311 worked.

Subsequently, the U.S. Congress amended Section 311 to make it even more readily available in cases of WMD proliferation. That occurred during the period of time that I was working for Majority Leader Frist, and I thought it was a sensible initiative at the time.

I do not believe that that authority has been used by the Bush administration since it was given to the Bush administration in September of 2006. But from my first-hand observation of the Chinese reaction the first time the Section 311 trigger was pulled in connection with proliferation, I think any suggestion by the Bush administration that they were thinking of using the expanded authority now available under Section 311 would certainly get the attention of financial institutions, not just in China, but in any country where proliferation is a problem.

[The statement follows:]

Prepared Statement of the Honorable Stephen G. Rademaker
Senior Counsel, BGR Holding, LLC
Washington, D.C.

Co-Chairmen Reinsch and Brookes, Members of the Commission, I am honored to appear again before you to discuss China's proliferation practices. When I last appeared here in 2005 I spoke on behalf of the Bush Administration; today I will speak on behalf of only myself. While my remarks today will be less authoritative, I will try to make them more interesting.

It has been two years since I was regularly reading the current intelligence on China's proliferation practices, so I must defer to others on the latest developments and trends in that regard. I think what I can most usefully present to the Commission is a description of what it was like as a U.S. diplomat to talk regularly to the Chinese government about arms control and nonproliferation matters from 2002 to 2006, and some of the principal conclusions I draw from that experience.

America's Nonproliferation Dialogue with China

As a U.S. diplomat, my engagement with China on these issues was—with one major exception that I will describe in a moment—with diplomats from the Chinese foreign ministry. Formal bilateral consultations on arms control and nonproliferation issues took place roughly twice a year, more frequently in Beijing than in Washington, but sometimes here as well. My Chinese counterparts were hard-working, earnest, and knew how to speak the language of nonproliferation.

In these consultations, the U.S. side would often present the basic facts of proliferation cases involving specific Chinese companies, and ask the Chinese side to investigate and stop the proliferation activity. Our Chinese counterparts would always appear to take the information seriously and promise to get back to us with their findings. In a number of cases, when they got back to us they said that they had confirmed our information and acted against the company in question. Usually this did not mean that someone had been prosecuted, but it did appear to mean that the company had been told to stop proliferating, and so far as I am aware, usually they did.

There was, however, a class of cases—what we came to refer to as the "serial proliferators"—where no

progress was ever made during my time at the State Department. Typically with regard to this class of cases, our Chinese counterparts would report back that they had been unable to confirm our information, that they were still investigating, and could we help them by providing more detailed information to substantiate our allegations? Often in these cases we would impose sanctions pursuant to the Iran Nonproliferation Act or similar legal authorities, which would lead the Chinese to complain that we were acting imperiously and without regard for Chinese sovereignty or goodwill. There was often the implicit threat that they might begin to withhold nonproliferation cooperation in other areas if we continued to act unilaterally against Chinese companies.

I may be reading something into these discussions that was not really there, but I often got the sense from body language and other nonverbal cues that our foreign ministry counterparts were uncomfortable talking to us about these cases. They conveyed a sense of pride and accomplishment when they could report to us that they had made progress on other cases. That same sense was always lacking in any discussion of the serial proliferators, for obvious reasons.

I never knew for sure what to make of the serial proliferator problem. I ultimately came to the conclusion that the companies in question probably enjoyed some sort of "protection" within the Chinese political system. Either they were owned or controlled by the People's Liberation Army, were closely connected to the Communist Party, or had some powerful patron somewhere within the government. Whatever the reason, it appeared to me that stopping the proliferation activities of these companies was beyond the bureaucratic power of our counterparts in the Foreign Ministry. In other words, by the time I left the State Department I had come to the conclusion that the problem with the serial proliferators was not that our nonproliferation counterparts within the Chinese government were uninterested in reining in these companies, but rather that they were unable to do so.

While this was frustrating, it nevertheless was, to my mind, a sign of progress. When I first began following these issues as a congressional staffer in the 1990s, I would not have said that there was anyone in the Chinese government who genuinely saw proliferation as a problem or cared to do anything about it. By the time I left the State Department I thought this had changed.

I would offer the same general characterization of China's cooperation with the U.S. Government in other proliferation-related areas during my time at the State Department. As you know, China has not been very helpful at the U.N. Security Council in ratcheting up pressure on Iran to comply with previous Security Council demands that Iran suspend uranium enrichment. Nevertheless, China has, at various times, provided unexpected help to the International Atomic Energy Agency in uncovering the history of Iran's nuclear activities.

With regard to the interdiction of proliferation-related shipments, China has rejected repeated U.S. requests that it join the Proliferation Security Initiative. On the other hand, there were times when, in response, to U.S. requests, China cooperated in particular interdiction efforts. There were also many times when China declined to cooperate. But the fact that China cooperated at all—and was willing to sustain the inevitable damage to its bilateral relations with the countries against which it was cooperating—was, to my mind, a promising sign.

What to Do?

While I believe we have made progress with China on nonproliferation issues, there obviously remains much room for improvement. We have no alternative, however, but to continue working with China in these matters. As we have seen with regard to proliferation activity by Chinese entities, it is possible to make progress through firm and patient efforts. With regard to these entities, I see two ways to make additional progress. One is to figure out how to empower those within the Chinese government who are prepared to work with us to stop proliferation. The other is to directly change the risk/reward calculus of

the Chinese entities in question.

I am not sufficiently expert on the internal dynamics of the Chinese government to make recommendations on how to strengthen one bureaucratic faction at the expense of others. As far as changing the calculus of Chinese entities, however, the record is clear that vigorous enforcement of U.S. sanctions laws and policies can make a big difference. U.S. sanctions may not make a big difference to individuals and to small enterprises that do not worry about their reputation and their ability to conduct business internationally, but sanctions can make a big difference to larger Chinese companies. Most of the serial proliferators from my time at State—companies such as China North Industries Corp. (NORINCO), Zibo Chemet Equipment Co., China National Precision Machinery Import/Export Corp. (CPMIEC), China Great Wall Industries Corp. (CGWIC), and Xinshidai—fall into the latter category.

The efficacy of U.S. sanctions is underscored by the State Department's testimony today that two of these companies—NORINCO and CGWIC—have in the past year begun a dialogue with the U.S. Government about how to avoid conduct that could result in their being sanctioned in the future. This is precisely the kind of result that U.S. nonproliferation sanctions laws are designed to achieve. The objective of these laws is not to punish foreign entities for proliferating, but rather to change the behavior of such entities so they do not proliferate in the first place. In this sense, the imposition of sanctions reflects a failure of these laws rather than a success. The Executive branch should continue to apply U.S. sanctions laws vigorously so as to encourage additional Chinese companies to follow the example of these two.

In this connection, I would also note that, in my opinion, we have only begun to explore the potential for financial sanctions to affect the behavior of proliferating entities. Two new tools were introduced during my time at the State Department that immediately got the attention of the Chinese. These were the issuance of Executive Order 13382 on proliferation financing on June 29, 2005, and the designation of Banco Delta Asia as a "primary money laundering concern" under section 311 of the USA Patriot Act on September 15, 2005. The Chinese government did not know what to make of these actions, but it found them alarming.

This was underscored to me in November 2005, when we had another round of nonproliferation consultations with the Chinese. For the first time ever, our foreign ministry counterparts were joined in these meetings by representatives of the China Banking Regulatory Commission and the People's Bank of China (i.e., the central bank of China). These banking officials were clearly eager to learn more about what we had done, what it meant for the ability of Chinese banks to do business in the future with entities that have been sanctioned by the United States for proliferation, and how great the risk was that Chinese banks themselves might be sanctioned by the United States.

With the assistance of the Department of the Treasury, we explained to these Chinese banking officials how the new U.S. tools worked and tried to answer their questions. They were surprised to learn, for example, that the freezing of assets under Executive Order 13382 extends to all financial transfers by designated entities, not just transfers that the U.S. Government can demonstrate were related to proliferation activity. They seemed especially worried about the broad authority available under section 311 of the USA Patriot Act, having seen how the application of this authority to Banco Delta Asia had had devastating consequences for that Macau-based financial institution.

Congress subsequently amended section 311 to make it more readily available for use against banks that conduct proliferation-related transactions. This was done in section 501 of the Iran Freedom Support Act, which was signed into law in September 2006. To my knowledge, this expanded authority has never been employed, but the prospect that it might be used would certainly get the attention of all foreign banks that service customers involved in proliferation. This in turn could compromise the ability of proliferating entities to conduct business through normal banking channels.

<u>China's Diplomatic and Economic Role</u>

In addition to doing more to restrain proliferation by Chinese entities, the Chinese government needs to do more diplomatically to help confront the hard cases in proliferation. I have been particularly disappointed by the level of cooperation China has provided with respect to North Korea and Iran. I do not share the Administration's optimistic assessment of Chinese cooperation in these two cases, and I do not expect us to be able to achieve acceptable diplomatic resolutions in either case until China agrees to do more.
With regard to North Korea, I will observe only that China has far more leverage over that country than anyone else, and it has consistently declined to bring that leverage fully to bear. The diplomatic course that we are on today with North Korea has as its premise—borne of nearly two decades of frustration—that China is simply unwilling to use all the influence at its disposal to require more responsible behavior by Pyongyang.

With regard to Iran, ideally the U.N. Security Council would continue tightening sanctions until the Iranian regime agrees to comply with the Council's demand that it suspend uranium enrichment activities. Russia has been the principal obstacle at the Council to the imposition of tougher sanctions on Iran, but China generally has backed Russia's position. Perhaps even more damaging, China has recently become much more aggressive in seeking to advance its economic interests in Iran. This has provided many U.S. allies in Europe and elsewhere with a new reason not to join in efforts to apply multilateral economic pressure on Iran outside of the context of Security Council-imposed sanctions. Why deny ourselves the benefits of trade with and investment in Iran, they ask, if the Chinese are going to simply step in and pick up the contracts that we walk away from? This concern on the part of our allies is not illogical, and is proving highly damaging to our efforts to build multilateral pressure on Iran.

China's aggressive pursuit of economic advantage in Iran is part of a larger pattern that we are witnessing in Sudan, Zimbabwe, Burma, and elsewhere. We can all appreciate the resource requirements of China's growing economy, but we are entitled to expect China to act more responsibly in all these cases.
Thank you.

HEARING COCHAIR REINSCH: Thank you very much. Mr. Sokolski.

STATEMENT OF MR. HENRY SOKOLSKI
EXECUTIVE DIRECTOR, THE NONPROLIFERATION POLICY EDUCATION CENTER, WASHINGTON, D.C.

MR. SOKOLSKI: Maybe it's because I've been out of government for a longer period of time, I get nervous so I am going to read my testimony. I find that the longer you're away from government, the more complicated things get. You read more. I'll try to keep this simple though.

First of all, I think the work you folks are doing actually is more important than even most people think. The oversight function in Congress is I think imploding, and so the importance of things like this Commission actually are going up.

They don't hold hearings, not routine ones, and certainly not on this series of topics, as much as I think they need to. So I feel

honored to be asked to come here.

I guess the message I'm going to try to convey today is everything you just heard, absolutely correct, but we're going to have to do a lot more and think bigger about the problem besides looking for violations of international and U.S. nonproliferation rules by the Chinese.

I think it would be nice if nuclear proliferators went out of their way to violate these rules, but I think they're getting smarter, so China doesn't really offer M-9 missiles to countries like Syria anymore. Why? Well, that would trigger sanctions.

On the other hand, Chinese front companies recently funneled North Korean-purchased dual-use nuclear goods to this Syrian reactor project. It's far harder to track and almost certain to go unsanctioned.

So should we reduce our efforts to monitor such transactions? I think as Steve laid out, of course not. But if you want to assure that we're doing all we can to reduce further Chinese-induced proliferation, I think you're going to have to track some additional trends.

Besides increasing covert and indirect strategic technology transfers to countries like Pakistan and Iran, we will now also need to worry about how Beijing might divide us from our closest Asian security allies. I'm talking about Japan, Taiwan, and South Korea -- governments that so far have skipped going nuclear or ballistic.

In addition what choices China makes to expand its domestic civilian and nuclear export programs will have a major impact on how much more nuclear weapons capable Pakistan, Iran, Saudi Arabia and other Middle Eastern states are likely to become.

Finally, whether and how China decides to increase its own nuclear weapons deployments will directly influence the weapons ambitions, not only of Beijing's East Asian neighbors, but of India, Pakistan, Russia, France, the UK, and the U.S.

This is another way of saying China now is a serious nation. It's not just a cheater; it's a player. So you have to worry about it as if it was more like Russia in an active sense. This gives rise, I think, to three suggestions.

By the way I go into great detail in the testimony on what they're doing in East Asia and the Pacific and other places, not so much to say oh, well, it's obvious they're going in a bad direction, but rather to show you what they're worried about and how contingent things are, and therefore it's worth watching these bigger trends.

In addition, I'm going to give you three big ideas, maybe a little wooly-headed, but I think important for modifying or adjusting our policies to deal with these bigger contingencies.

First, I think we need to encourage China to cap its further production of nuclear weapons usable fuels. Our current policies are

nearly doing the reverse. On the one hand, our Department of Energy is actively promoting uneconomical commercial spent fuel recycling projects and the use of near-nuclear weapons-usable plutonium-based reactor fuels domestically, as well as in Japan, South Korea, and with this most recent nuclear cooperative agreement in Russia.

Our U.S. State Department, meanwhile, is doing little to pressure China to announce that it will no longer produce fissile materials for military purposes, even though the other Permanent Members of the U.N. already have.

The indirect compound effect of these two policies of the U.S. is to foster the continued growth of a nuclear powder keg of plutonium in the Far East, one that is sure to have negative knock-on effects on India and Pakistan's own nuclear weapons aspirations.

It would be preferable for China to announce that it will suspend any further production of fissionable materials for military purposes. By the way, most experts say they don't make it anyway. So making the announcement, you would think, would not be heroic. That would be preferable. And that it shelve its immediate commercial plans to produce plutonium-based fuels for its breeder reactor and its light water reactor programs. It's not necessary.

They can have nuclear power without those dangerous fuels. This, in turn, could be used to pressure Pakistan and India to swear off making fissile materials for military purposes, something our government claims it's dedicated to doing. That's our policy. We want India and Pakistan to make that announcement too.

To leverage such results, Washington might suggest that Japan simultaneously suspend its own uneconomical production of plutonium-based reactor fuels at Rokkasho-mura and defer all U.S. government-funded efforts to do so domestically.

We have programs that Congress is looking at spending more money to make plutonium-based civilian reactor fuels which are grossly uneconomical. To do so jointly with Russia, which is part of this 123 Agreement that's being announced--I think it was announced last week--and bilaterally we have a program with pyroreprocessing with South Korea, which has got everybody looking at everybody nervously.

Let me go over the last two and stay within limit. I've got 51 seconds. I think we should encourage China only to push nuclear projects that are unambiguously profitable. By the way, if we ask them to do it, we might think about doing that ourselves. We are subsidizing the daylights out of our own nuclear programs. Now, admittedly we're doing this also with non-nuclear programs.

We need to stop piling on these subsidies and we need to get certain principles that are embodied in international agreements we

claim we back, called the Charter Energy Treaty and the Global Charter for Sustainable Energy Development, to be the new norm, and that norm would be state the full price of things, compete them openly internationally, and that goes for energy projects.

As we move, as apparently all three of the candidates for president say we're going towards a post-Kyoto Protocol protocol, we're going to want to do this anyway. We're going to want to have open market competition and try to figure out how to lower carbon emissions the most economical way.

Finally, I recommend in here that henceforth the U.S. should discourage state transfers of nuclear weapons to other state soil in peacetime. Why? The Pakistanis have approached me privately. They want to know if there are some things the United States would do if Pakistan did something different with regard to its nuclear weapons arsenal?

And the only idea that I could come up with is would they promise not to transfer nuclear weapons to Saudi Arabia if we promised not to transfer any more nuclear weapons to Europe and actually reduced our own tactical deployments. They expressed some interest in that.

I think we need to start thinking about the contingencies of China and Pakistan moving weapons to other countries' soil like we did in the '50s because they're talking about it, and that will produce a real problem.

One final comment and then I'll close out. I did go over the limit. I apologize. All of these policy adjustments should be taken in addition to the kinds of things that Steve raised. Certainly if we fail to take these additional steps I lay out, I think China will keep pressing its own nuclear policies domestically in East Asia and Middle East in a way that will come in direct collision with our security interests.

Fortunately, none of the adjustments I recommend entails much risk. All of them can be begun and even completed without negotiating new treaties. Each would save millions or even billions of dollars of wasteful government spending and I think they all would make us safer.

With that, I conclude. Thank you.

[The statement follows:][2]

Panel V: Discussion, Questions and Answers

HEARING COCHAIR REINSCH: Thank you.

---

[2] **Click here to read the prepared statement of Mr. Henry Sokolski**

Commissioner Fiedler.

COMMISSIONER FIEDLER: Thank you.

Let me return to something from the previous panel, which is the question of Chinese government involvement in its companies' proliferation. I understand the diplomatic or perhaps understand the diplomatic necessity of avoiding the question directly of whether the Chinese government is letting this happen or not, in other words, allowing the fiction of--the persistent fiction of government entities constantly violating.

NORINCO isn't a little actor. So seven times being sanctioned indicates the Chinese government didn't crack down on them and allowed it to continue to happen.

Now, the question becomes is it just somebody else doing it? And so do we have anything but a short-term solution to the problem via the sanctions which I endorse? I just don't endorse their effect all that much; I mean their long-term effect all that much. So let's discuss government culpability here in reality as opposed to diplomatically. Iran--you know.

MR. SOKOLSKI: My approach in the testimony is to try to lay out why the government of China has an interest in helping out with missiles and nuclear-capable systems. It's pretty clear in each case what it is. Because of that, I think the odds of the government not being aware of the activities, even of small front companies, is probably pretty low--

COMMISSIONER FIEDLER: Yes.

MR. SOKOLSKI: --because it makes sense. It's not errant behavior. It's consistent with certain dominant interests. I think unless you can approach the government and make clear to them why it might make more sense to do something differently or put their thinking in some other context they hadn't thought about, you may not get much traction.

COMMISSIONER FIEDLER: Mr. Rademaker. I'll come back to you.

MR. RADEMAKER: Thank you. Let me concede at the outset that I do not know the answer to your question. I think it's an important question. I think it's certainly the case in the past that as a matter of strategic interest, the Chinese government must have condoned certain types of proliferation. I cannot believe that M-11 missiles were shipped to Pakistan by some rogue corporate entity that was out to make a fast buck.

I can't believe that the nuclear weapons design with Chinese characters found in Libya slipped out of China. I think there was a period when certainly the Chinese government was condoning, and presumably not just authorizing, but actually making these transfers.

I'm not aware that there is a lot of evidence of that kind of activity today, strategically based proliferation by the Chinese government. What we have instead are instances in which corporate entities have been engaging in proliferation, and your question is are they doing this as an economic matter to make money or is this just a new form of a government policy that permits them to go forward?

I don't know, but I would make a couple of observations. First, I think China is a big country and it's a big government, and even though there is one-party rule, I don't think that means that it's North Korea. In North Korea, there's one man whose word is the law, and everything pretty much follows from him. I've never had that sense in China that there is that degree of centralization where everything goes back to a single decision-maker.

If that were the case, I'd like to know who he is because we could go talk to him about proliferation. My sense is that there are discrete power centers in China, and as I explained in my testimony, my fundamental take on what's been happening in recent years in the proliferation area is that there's not full agreement among these power centers about what to do. Some are more willing to see things our way than others. In some cases, those who see things our way seem to get the upper hand and transfers get turned off, and in other cases, they seem not to get the upper hand, and transfers don't get turned off.

I suppose you could say that in those cases where transfers don't get turned off, the government is condoning it. I guess there is no other way to interpret that, but I think it's a little bit different than in the past when it would appear there was a clear, affirmative decision by the the government writ large to engage in proliferation.

I think what may be happening now is that in certain cases, as I suggest in my testimony, because of the backing of powerful patrons, certain companies are able to continue to proliferate because nobody is in a position to say they can't. And what we'd like to do is change that, and ideally the way we would change that is by getting the ear of all these power centers in the Chinese government and persuading all of them that it's in their national interest to stop this kind of conduct.

As I point out in my testimony, I think we have made progress over the last ten or 20 years. When I first began covering these kinds of issues as a congressional staffer--it will soon be 20 years ago--it was not my view that anybody in China really cared to stop proliferation. I think that's different today. I think there's been considerable evolution in China, and today there are certainly people within the government in key positions who would stop this if they could.

So that's considerable progress from where we've been, and what we would like to do is make sure that progress continues to a logical

conclusion where the entire government is on board with the importance of this as a national policy.

But we're not there yet, in my judgment, and until we get there, the best tool I'm aware of is the continued application of our sanctions laws which in at least some cases seem to be changing the risk-benefit, risk-reward calculations of economic enterprises.

Unless I'm misreading Secretary McNerney's testimony, NORINCO did not come to the U.S. government because they were being pressured by the Chinese government to talk to the U.S. government. My reading of her testimony is they made an economic judgment that as an enterprise, they were losing money because of U.S. sanctions and they wanted to do something to fix that.

So until we get to the point where the Chinese government as a whole is committed to doing the right thing in every case, sanctions appear to be the best tool that we have to address the remaining problems on a case-by-case basis.

COMMISSIONER FIEDLER: Thank you.

HEARING COCHAIR REINSCH: Thank you.

COMMISSIONER FIEDLER: I'll come back on a second.

HEARING COCHAIR REINSCH: If we have one. Commissioner Mulloy.

COMMISSIONER MULLOY: I've read your bios. You both have really done a lot of great work for the Republic so we thank you both for distinguished service.

I wanted to ask you both this question. Mr. Rademaker, maybe you first. Ms. McNerney talked about that the U.N. Security Council had agreed to put sanctions on Iran to help persuade Iran not to pursue the nuclear weapons development. Is, as far as you can tell, is China living up to the obligations that it assumed in voting for those sanctions in the Security Council?

MR. RADEMAKER: I don't personally have any information to suggest that they are violating the legal obligations that they have under existing U.N. Security Council resolutions.

One of the points I make in my testimony, however is that China has been unhelpful in helping us bring to bear maximum economic pressure through the United Nations Security Council. They've never exercised their veto, which I guess would be clear proof that China was preventing more serious action by the Security Council, but my understanding of the dynamic within the Security Council is that Russia has on occasion threatened to veto more serious action, and by all appearances, China was supportive of Russia's position in those discussions.

So I think the complaint that I have about China and Iran on the diplomatic level these days is that they, well, my complaint is twofold.

First, that they are not supporting our efforts and those of like-minded Western countries on the Security Council to persuade the Council to take more serious action that would get Iran's attention and perhaps make a difference, perhaps give the Iranian government reason to rethink its nuclear policies.

But then, secondly, an additional point that I make in my testimony, China increasingly is pursuing its own economic advantage in Iran, and this has become the leading explanation that one receives these days from our European allies when they are asked why don't you act either unilaterally or multilaterally with us to impose additional measures on Iran outside of the Security Council?

Assuming we continue to have problems persuading Russia and perhaps China to agree to more meaningful Security Council action, let's act on our own to make Iran pay an economic price. Let's curtail investment. Let's curtail trade credits.

The European governments continue to subsidize both investment and trade with Iran, and the justification or the rationalization that one often hears today from Europeans for their continued pursuit of those kinds of policies is, what would be the point of our giving up those markets or foregoing those investments because we've seen when we pull out, the Chinese immediately step in?

I don't happen to agree that that's a sufficient reason for the Europeans not to do more, but I would accept that there is a certain logic to the position, and our ability to multilaterally impose meaningful measures on Iran in concert with our European allies and the Japanese is very much undermined if China for reasons of economic self-interest is going to step in every case and replace the investment or replace the trade that we want to withhold.

COMMISSIONER MULLOY: Good. Mr. Sokolski.

MR. SOKOLSKI: I think it's even worse than that.

COMMISSIONER MULLOY: No, but are they violating?

MR. SOKOLSKI: Let me answer. First, if you take a look at the sanctions, they are in some instances specific enough never to be violated and vague enough never to be enforced. So first cut, you're probably not going to get anybody red-handed on this one. So that's point one.

I'd say it's worse than even Steve has laid out because the Chinese have made a lot of bad investments in Iran. It's kind of like American companies that overinvest technology in China and they have to get their money out, and it takes awhile. They've done the same thing in Iran, mostly because the investments are being dictated by this desire by the state to have a strategic connection with Iran.

Well, but it has this perverse effect. They have to somehow get leverage over the Iranians. One of the ways to do this is to have trade

that is critically dependent on the Chinese supplying certain things.

Now, they're going to be very careful to fly below the radar screen as much as possible of anything that's sanctionable activity. I mean this example I used in my oral presentation just at the beginning goes to this. Front companies that acted as brokers for the North Koreans to get items to the Syrian reactor project, the folks that were interested in that project know how important those front companies were. Did they violate any rules? No.

So they're going to have an interest to continue to do this. Tiananmen Square and the sanctions that followed from Tiananmen Square are very much on their mind and why they are so aligned with the Russians in opposing sanctions. When you put those factors that I've laid out all together, it suggests a kind of prevailing strategic interest in playing the game at the margin.

So we're going to have to be more clever in identifying what's sanctionable, number one. Number two, we're going to have to try to figure out how to get the Chinese interested in something other than just getting their money out of Iran, and finally, I think we're going to have to just more generally impress upon them how risky this business is.

HEARING COCHAIR REINSCH: Thank you.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you.

I want to challenge two items, Mr. Sokolski, not in a big way. You said that China wants to get its money out of Iran. I believe they're going to get oil out of Iran, and so there is a long-term economic benefit for what they're doing. Their MOU relating to access to the fields is I think rather aggressive, as I understand it, number one.

Number two, you said early on in your testimony that China should move towards a more profit-based approach as it relates, I believe, to nuclear power development, et cetera, and I'm reminded I believe it was of Jim Fallow's book many years ago, More Like Us, that we continually have this mind-set that we want to impose on China as to how they address things. It's a non-market economy. Profit is at times an alien concept to how one develops economic models there.

So challenging those two issues. But more importantly, and the question was made of the earlier panel I believe by Mr. Shea, Commissioner Shea, what additional tools rather than just operation under the current tools--you've talked about specificity, et cetera--what additional tools do you think we should be looking at, Congress should be looking at, to give to the administration, if any, to enhance our success in this important area?

For both witnesses, that last question.

MR. SOKOLSKI: Since I'm challenged--

COMMISSIONER WESSEL: Challenged in a non-confrontational way, if you will.

MR. SOKOLSKI: Okay. Well, let me answer in a nonconfrontational way.

COMMISSIONER WESSEL: Yes, please.

MR. SOKOLSKI: Yes. They want to get the oil. The question is when are they going to get it and at what cost? And so far, it's a long ways away and costs lots more than they hoped it would. It's one of the reasons things aren't working out quite as well as they want.

COMMISSIONER WESSEL: Okay.

MR. SOKOLSKI: With regard to More Like Us, it's a fair point. However, it's not like we're doing much in the way of market mechanisms to make big energy capital construction decisions these days. I mean after the catastrophic California experience, we've been racing perhaps too much in the opposite direction of trying to--

COMMISSIONER WESSEL: No argument with regard to what we do here.

MR. SOKOLSKI: Yes.

COMMISSIONER WESSEL: And the failure of an energy--lack of an energy policy.

MR. SOKOLSKI: No, no. I'm rather suggesting that we have perhaps too much of a desire to follow the models. As one industry wag at the Nuclear Conference I was at recently said, we need to follow the Russian and the French model and the Chinese model, variously Mao, Stalin and Louis XIV. I'm against it.

But that said, I wouldn't suggest that they follow us. And that wasn't my suggestion. Because I don't think we're doing very well here. I think, think of the follow-on to Kyoto as a problem for everybody, that people are going to have to, as governments, come to conclusions about what they're going to invest in to reduce their emissions.

You want people to make the decisions on the basis of what's quickest, cheapest. It's a compound. So you're not interested in lunar power, for example, even though it might be the cleanest but it's neither quick nor cheap.

To make those decisions, it would be useful if the international norms, not American norms, of open bidding and international competition and clearly stating as much as possible what things cost, was something we encouraged.

The more we do that, the better whatever the result is likely to be, and if something is dumb, it will become evident that it's dumb quicker and then you can make a change.

COMMISSIONER WESSEL: No argument there.

MR. SOKOLSKI: In answer to your question, I think the single-most important thing Congress could do to give our executive branch the tools it needs is less money. This is counterintuitive. I think when you keep sending money to the Energy Department, it keeps coming up with ideas of how to spend it that don't make sense.

It would be helpful to send less. And particularly, the programs that they're engaged in with South Korea, with this pyroreprocessing program, which is really just some additional steps to regular reprocessing, is making it very clear that we're prepared to see South Korea come very near nuclear weapons technical capability.

Similarly, the money that is being proposed to be spent on the Global Nuclear Energy Partnership with Russia on fuel-making activities that are uneconomical in the extreme probably doesn't do anything to discourage China to think about what it's doing that's similar.

And then finally I think the biggest incentive, separate from what we give tools to our government to do, I think Japan is in a real bind right now. It has spent $20 billion on a single plant to make--I mean it's just an enormous amount of separated plutonium per year. I think in the testimony I have the figure. It's mind-boggling.

If you hold on, it's mind-boggling enough I want to actually cite it here for the record.

COMMISSIONER WESSEL: 2,000 tons; is that the--

MR. SOKOLSKI: Well, hang on here. Let's see here.

COMMISSIONER MULLOY: 20 billion.

MR. SOKOLSKI: Well, that's the amount for the plant, but the amount of separated plutonium this thing produces per year is equally as interesting. Here we go. Right. It produces five metric tons of separated plutonium annually. That's enough for a thousand nuclear weapons per year.

Now, if you think for a moment that the Chinese don't pay attention to that, you haven't been reading the news. The Chinese have volunteered that they don't want to engage in a nuclear arms race in the region. What's that about?

Partly this. It would be nice to give Japan some way to reasonably back off this project and give China some reason why it doesn't have to go forward copying the Japanese, and for us perhaps not to go down this road as much as the Department of Energy is encouraging us to do.

I think it's along those lines that you want to see trends move in a different direction because where we're headed is a competition in that region and beyond that will end up making us having to arm more in the nuclear arena which is really quite stupendous. I mean we

haven't done that since--I don't know--when was the last time we made a nuclear weapon? I mean it's 1980 something.

MR. RADEMAKER: Depends on your definition of--

MR. SOKOLSKI: Well, it's been awhile, and best not to go back to that, I think. Yes.

HEARING COCHAIR REINSCH: Okay. Thank you very much.

Commissioner Slane.

COMMISSIONER SLANE: Thank you. Isn't this really all about China's overwhelming demand for resources and their drive to capture resources, and as the demand will continue, in my opinion, as their middle class grows, the problem that we're talking about today is going to get worse?

MR. RADEMAKER: Commissioner, I guess I wouldn't agree that everything is about the resource issue, but I do in my testimony advert to the fact that the policy that we currently see, that I just complained about, of China stepping in to gain economic advantage in Iran, when in those cases where Europeans or others pull out, there are analogs to that in other countries--Sudan, Zimbabwe, Burma--where China is taking advantage of the fact that these are essentially pariah regimes that no one in the rest of the world will deal with economically.

And they are stepping in to win oil concessions, mineral concessions, invest, and otherwise take advantage of the absence of competition, and it would appear that the explanation for this is precisely as you suggest, that they've made a strategic judgment that with their growing economy and their voracious appetite for oil and mineral resources to fuel that economy, they need to step into the international arena and invest and develop relations even with pariah regimes, and that is, in fact, a huge problem.

It's a huge problem for the policy we are currently pursuing with our allies to persuade Iran to abandon its nuclear weapons ambitions and it's a problem to the extent we're trying to do something about the situation in Darfur or we're trying to do something about Mr. Mugabe in Zimbabwe, and in every case the explanation is the same.

I think on the question of what to do about it, China needs to be persuaded that whatever very narrow economic advantage it might gain by taking advantage of the political situation in these countries to ingratiate itself with an unsavory regime, they will pay a higher price in other areas for having done so.

MR. SOKOLSKI: If I may, I think that last point is very important. I spent a week at RAND with some officials from the People's Liberation Army, and we were trying to explain to them that when they went out and captured markets, as you describe, and got these long-term contracts, all they were doing was making it more expensive in the long haul for them to extract those resources than it

would be if they put more faith in sort of the international market for whatever that resource was.

Now part of it is a distrust of the international market. They feel like they can't play, and you'd have to ask experts about that and as to what can be done or not done and why things are done and why they feel that way. But generally, we fought the Second World War, last I checked, to make everybody have access to everybody else's markets rather than to try to have energy independence or food independence along the lines of Hirohito and Hitler who decided the only way to do that was to invade the world.

We have an interest in them seeing the profit of relying on the market, and I think that is a separate line of inquiry I'm not the expert to go into this, but that's what you would want to get more information on: how do you persuade them that they're actually making life more expensive for themselves when they proceed the way they do in capturing markets?

COMMISSIONER SLANE: I completely agree with you. But what worries me is if we don't form some cooperative agreement or convince them that there's another way to go, that this situation is just going to get worse.

MR. SOKOLSKI: It might, yes.

HEARING COCHAIR REINSCH: Thank you.

Mr. Sokolski's testimony reminds me of a simulation game I played the weekend before last, which concluded with a reunified nuclear Korea under a military government and a nervous Japan that had made a deal with the Russians to acquire nuclear weapons, which was not the world that we anticipated at the beginning of the game.

Mr. Rademaker might be interested to know that all those things happened after we had elected Gardner Peckham president of the United States, although I wouldn't say that he gets the blame for that particular conclusion.

That was apropos of nothing except to say that I think your point about the consequences of not thinking through a proliferation policy are well taken, and that there is a wider variety of outcomes out there than people might think.

In the game context, which took us 16 years into the future, it was not entirely an unrealistic conclusion given what had happened in the previous 12 years that I didn’t talk about.

Let me ask in that context, Mr. Sokolski, kind of an errant question but one I think you might want to comment on, which is the Indian nuclear deal from a proliferation standpoint. Do you have a view about that? I would assume you do.

MR. SOKOLSKI: I'm going to try to restrain myself.

HEARING COCHAIR REINSCH: Well, in a hundred words or

less.

MR. SOKOLSKI: Well, emotional outbursts will be repressed as well. It was a very unnecessary agreement, one that we did not need to do to promote good trade or good relations with India that weakened the nuclear rules even more. And that's not great.

Now, my hunch is, is that we're going to have to repress the spread of nuclear technology and even nuclear capable missiles with reference to economics more as a result of what we did there.

What I'm trying to say is we have relied on the NPT, Nuclear Suppliers Group, Missile Technology Control Regime, you know, all the things that you and I used to struggle with when we were in government, right, to somehow either restrain trade in these dangerous technologies or at least give the appearance of restraint.

That's not looking so good. It's kind of fraying and partly because of the Indian deal and deals like it. Where I think we're going to have to pay more attention therefore, besides not weakening these things any further and trying to shore them up, is to try to figure out where God's invisible hand is trying to help us.

Where things are grossly uneconomical as compared to their alternatives, where those things are dangerous, we need to be pointing that out. We need to stop spending extra money on those things and promoting their export. I think if we do that, we may still be safe, but if we don't, the rules as a result of the Indian agreement have taken quite a hard, solid hit.

They've been worn down over the years previously, but this was kind of an additional slap in the face, and so it's going to make it more important to do these other things than ever before.

HEARING COCHAIR REINSCH: Thank you. And I think on that note, let me thank our witnesses and all the panels for a very useful and informative hearing, and we're adjourned.

[Whereupon, at 4:05 p.m., the hearing was adjourned.]