DEVELOPMENTS IN CHINA'S CYBER AND NUCLEAR CAPABILITIES

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY

REVIEW COMMISSION

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 26, 2012

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: 2012

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Hon. DENNIS C. SHEA, *Chairman*
Hon. WILLIAM A. REINSCH, *Vice Chairman*

Commissioners:
CAROLYN BARTHOLOMEW
DANIEL A. BLUMENTHAL
ROBIN CLEVELAND
Hon. C. RICHARD D'AMATO
JEFFREY L. FIEDLER
Hon. CARTE GOODWIN
DANIEL M. SLANE
MICHAEL R. WESSEL
LARRY M. WORTZEL, Ph.D.

MICHAEL R. DANIS, *Executive 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 the 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 Nol. 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.

April 4, 2012

The Honorable Daniel Inouye
President Pro Tempore of the Senate, Washington, D.C. 20510
The Honorable John A. Boehner
Speaker of the House of Representatives, Washington, D.C. 20515

DEAR SENATOR INOUYE AND SPEAKER BOEHNER:

We are pleased to notify you of the Commission's March 26, 2012 public hearing on "*Developments in China's Cyber and Nuclear 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.

At the hearing, the Commissioners heard remarks from former Vice Chairman of the Joints Chiefs of Staff Gen. James Cartwright (USMC, Ret.), now Harold Brown Chair of Defense Studies at the Center for Strategic and International Studies, and testimony from three panels of expert witnesses.

Richard Bejtlich of Mandiant, Nart Villeneuve of Trend Micro, and Jason Healey of the Atlantic Council discussed trends in Chinese computer network exploitation. Mr. Bejtlich and Mr. Villeneuve described their research on persistent cyber espionage "campaigns" targeting businesses, government entities, and nongovernmental organizations. Mr. Healey described a framework for holding nationas accountable for malicious cyber activity emanating from their borders.

Henry Sokolski of Nonproliferation Policy Education Center and Dr. Phillip A. Karber of Georgetown University discussed Chinese fissile material production and methods of concealing nuclear materials. They testified that China's secrecy on nuclear matters has caused considerable doubt about the size and nature of its nuclear stockpile.

A panel on Chinese nuclear forces and strategies included Dr. Mark Schneider of the National Institute of Public Policy and Dr. Phillip C. Saunders of the National Defense University, with Mark Stokes of the Project 2049 Institute providing written testimony for the record. The witnesses described the evolution of Chinese views on nuclear war fighting and the implications for the United States.

Finally, Representative Frank Wolf presented remarks on the potential dangers of Chinese telecommunications equipment.

We note that prepared statements for the hearing, the hearing transcript, and supporting documents submitted by the witnesses will soon be available on the Commission's website at www.uscc.gov. Members and the staff of the Commission are available to provide more detailed

briefings. We hope these materials will be helpful to the Congress as it continues its assessment of U.S.-China relations and their impact on U.S. security.

The Commission will examine these issues, along with other topics enumerated in its statutory mandate, in its 2012 Annual Report which will be submitted to Congress in November 2012. Should you have any questions regarding this hearing or any other issue related to China, please do not hesitate to have your staff contact our Congressional Liaison, Jonathan Weston, at (202) 624-1487 or via email at jweston@uscc.gov.

Sincerely yours,

Dennis C. Shea
Chairman

William A. Reinsch
Vice Chairman

This transcript has been amended based on clarifications submitted by Commissioners and witnesses.

CONTENTS

MONDAY, MARCH 26, 2012

DEVELOPMENTS IN CHINA'S CYBER AND NUCLEAR CAPABILITIES

Panel I: Cybersecurity

Panel II: Fissile Material Production and Nuclear Cooperation

Panel III: Nuclear Forces and Strategy

Additional Material Submitted for the Record

DEVELOPMENTS IN CHINA'S CYBER AND NUCLEAR CAPABILITIES

MONDAY, MARCH 26, 2012

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in the Hylton Performing Arts Center of the George Mason University Prince William Campus, Manassas, VA at 9:30a.m., Chairman Dennis C. Shea, and Commissioners Jeffrey L. Fielder and Larry M. Wortzel (Hearing Co-Chairs), presiding.

OPENING STATEMENT OF COMMISSIONER JEFFREY L. FIEDLER HEARING CO-CHAIR

HEARING CO-CHAIR FIEDLER: Welcome, everyone. My name is Jeff Fiedler, co-Chair of the U.S.-China Economic and Security Review Commission's hearing on "Developments in China's Cyber and Nuclear Capabilities."

We have some excellent witnesses joining us today to provide testimony about China's evolving strategic capabilities.

Before we begin today's panels, we're honored to receive opening remarks from former Vice Chairman of the Joint Chiefs of Staff and current Harold Brown Chair in Defense Policy Studies at the Center for Strategic and International Studies. General James Cartwright. Welcome, General.

General Cartwright really needs no introduction. However, I'd like to note that this is his second appearance before the Commission. I think it's fair to say that his first testimony back in 2007, while serving as head of U.S. Strategic Command, was an inflection point for the Commission's work on cyber.

Over these past five years, we've placed greater and greater emphasis on cyber-related issues, a trend we continue with today's hearing. It's clear that the General's impact on the U.S. military was the same even as he divided his time among issues ranging from missile defense to the war in Afghanistan.

General, on behalf of the Commission, I want to thank you for your distinguished service and your participation here today. We look forward to your remarks, and I don't know if you can top your last statement when you were before us that cyberwar was a weapon of mass destruction.

Thank you, sir.

PREPARED STATEMENT OF COMMISSIONER JEFFREY L. FIEDLER
HEARING CO-CHAIR

Welcome, everyone. I'm Commissioner Jeffery Fielder, co-Chair of the U.S.-China Economic and Security Review Commission's hearing on "*Developments in China's Cyber and Nuclear Capabilities*." We have some excellent witnesses joining us today to provide testimony about China's evolving strategic capabilities.

Before we begin today's panels, we're honored to receive opening remarks from former Vice Chairman of the Joint Chiefs of Staff, and current Harold Brown Chair in Defense Policy Studies at the Center for Strategic and International Studies, General James Cartwright.

General Cartwright needs no introduction. However, I'd like to note that this is his second appearance before the Commission. I think it's fair to say that his first testimony—back in 2007 while serving as head of U.S. Strategic Command—was an inflection point for the Commission's work on cyber. Over these past five years, we've placed greater and greater emphasis on cyber-related issues, a trend we continue with today's hearing. It's clear that the General's impact on the U.S. military was the same, even as he divided his time among issues ranging from missile defense to the war in Afghanistan.

General, on behalf of the Commission, thank you for your distinguished service and for your participation here today. We look forward to your remarks.

OPENING STATEMENT OF GEN. JAMES CARTWRIGHT (USMC, Ret.)
SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL TUDIES

GENERAL CARTWRIGHT: I'll try to not be so controversial this time around.

COMMISSIONER BARTHOLOMEW: Oh, we like it.

HEARING CO-CHAIR FIEDLER: Please do.

[Laughter.]

GENERAL CARTWRIGHT: I would like to take just a few minutes on both the cyber issue and the nuclear issue if that would be okay.

HEARING CO-CHAIR FIEDLER: Please.

HEARING CO-CHAIR WORTZEL: That would be great.

GENERAL CARTWRIGHT: Just to give you some thoughts on both of them. I think one of the things that's becoming evident, particularly since the last time that I had a chance to talk with the Commission, is that the concerns that we have in cyber with the Chinese really do rise to the level of national security issues, in particular, the potential threat and theft of intellectual capital, and that constant and persistent threat, that while it's very difficult in cyber to have a smoking gun, so to speak, the clear paths back into servers and other mechanical devices inside of the Chinese sovereign domain remains a constant problem for us.

And so I think one of the things that I'd like to highlight here is that we have to find a dialogue to address these issues, and my preference, my recommendation, my personal opinion, is that that does not need to be a military dialogue. It really needs to be a whole government dialogue that is more comprehensive than what would occur in a mil-to-mil channel although having a mil-to-mil dialogue is probably not a bad thing.

What we are watching and what we are concerned about are the potentials for several different vectors to be used in cyber to come into the United States. Whether it be for acts to gain knowledge and intellectual capital, whether it's in the industrial area, or in defense, it really doesn't matter. It is still a national security issue when you look at the intellectual capital that is being exfiltrated out of the United States.

We worry about the potential of our equipment through the supply chain to have been tampered with, and that that equipment could potentially hold zero day exploits, things like that, whether they be on the IT side of the equation or whether they be in other domains inside of various companies.

The second area that is probably very concerning to us is the wired area. In other words, the ability to come in and start to query directories and whatnot of files on computers whether those computers be inside of companies,

inside of education organizations, governmental organizations. All of those things have information that when put together starts to build a story, starts to give you a path and an understanding of how people think about things and also about the intellectual properties that people have that might be of value.

I think the third area which is the most troublesome for the Department of Defense is the wireless approach, and this is the ability to get into what people will think about today as more things like iPads and telephones and whatnot, but really what you're saying here is that any aperture that's out there is a target.

Those apertures can be on military systems, whether they be missiles or airplanes or ships or ground systems. Those apertures can obviously be in embassies and all over the country, and so these kinds of accesses are troublesome because at the end of the day, whether you're traveling through fiber or copper or through the air, it's just a waveform on which there's generally some sort of a vehicle, a truck, let's call it, that carries something that is as innocuous as, you know, where am I and what am I doing and what's the environment here and what the directories files look like, to going inside the guts of an airborne radar and looking at the buffer and overflowing it or doing things like that, things that are systems that we count on day in and day out.

The idea and the concern that thinking along those lines, imagine an airliner, imagine what you could do on the inside of an airliner. An airliner today is full of apertures. They bring on board phones, computing WiFi, et cetera. That's an open door into the system.

Now, it doesn't necessarily need to be the nation state. It doesn't necessarily even need to be sponsored. But the opportunity there is significant, and so thinking about those as forms of conflict. From the department's standpoint, we rely on those apertures. We are very interconnected. Our leverage is our ability to do work in environments and to coordinate between the activities through command and control systems. Those systems are vulnerable.

And it's not to say that any adversary wouldn't be thinking along those lines, but the work that we've seen from the Chinese would indicate that they are thinking along those lines, and that this is a threat that we're going to have to understand and will persist.

The last thing I want to do in this is to demonize the Chinese. That's not of anybody's benefit and oftentimes becomes a self-fulfilling prophecy, and I worry about that, but there has to be a way to have dialogue. There has to be a more robust dialogue.

My preference, my recommendation to the Commission, is that dialogue should not be through the military, as I said before. That should be a governmental activity, government to government. It has to include the private sector, but it should be done on a concept of whole of government, not on a pure

defense construct, and so I really think that each of these avenues of approach--and there are others. There's close proximity type ways with thumb drives and things that people can get in and jump across air gaps, things like that.

But this is a country that prides itself on limiting access to the networks. So to say that they don't have control is somewhat problematic for me.

The second area here is that as you think about cyber, I mean this is an international forum. Okay. It still requires some bilateral work, but it needs to be multilateral in the end to understand where we're going and how we're going to do this, and you've got to think about it in a multilateral format, and in that discussion there are certain things, certain rights and certain responsibilities that come with those rights.

If you're going to work in this environment, if you're going to use this environment, it's a wonderful environment. It's highly leveraging. It has done so much for our business concerns all over the world to give us capability and advantage when we can get it and for us to work in an international forum. But with that comes responsibilities. With those rights come responsibilities.

From a military standpoint, we try to understand what's an appropriate response to these types of activities. Certainly when you start, you want to be working on the Article 3 side, the normal legal side, looking at this more as a crime type activity, and as you do so, trying to understand what precedents you set, how you get attribution, and how you then proceed to do whatever needs to be done to first stop anything that's going on.

If you have a server that's spewing malicious code, to get that stopped and get it stopped in hours, not days and weeks. Then the next thing is to try to understand was this something that the server, whoever owned the server, intentionally did? Were they the victim of a third-party, whether it be somebody from the government or somebody, a private interest inside in that country, or was it somebody outside that country just using them as a vehicle to get into you?

I mean all of those are possibilities. All of those need some sort of a formal approach to be able to deal with and to work your way back through the forensics of that kind of activity.

But what you have to deal with, and what we have to deal with, I think, or what the military has to deal with is the immediacy. So this is not unlike the current laws that exist. Stop the threat.

Now there's plenty of ways to do that. Heretofore, during my time in the government for the last four or five years, the first thing we did was go to the State Department and say this server in this country is putting out bad information. Go to that country and ask them to stop in 48 hours. We're not judging them. We're not judging whether they're the guilty party. Just stop it.

Now, we've never had a country refuse to do that that I'm aware of.

But if they did, then you can invoke the right of self-defense. The question is what should that look like? My thought process up until now has been that that server then without collateral damage around it is fair game to stop wherever it's located because you gave the country fair notice, stop it.

That doesn't mean you've eliminated the threat. These things go all over the place, but it does mean that you have a venue by which you can say that specific server was causing me problems, we complained, nothing was done, stop it, and we have the tools to do that and to do that just to that server.

Again, we've never had that problem. We've never had a nation state turn around and say no, we're not going to stop it. But it's that thought process.

How are we going to actually make that policy and legislate that kind of activity? You know, what is the right of hot pursuit in these environments? Is it one server? Is it two servers back? What's fair notice? What's declaratory policy look like? I think these are all things that we have to start to get our mind around, but it should not be unilateral.

It should be done in a collaborative fashion on an international basis, you know, first with our friends, and we have undertaken, the government has undertaken the work to go to the Five Eyes construct in the intelligence community because we have intellectual and classified exchange activities there that are sanctioned, and we can move data back and forth. We can talk about things that we may not talk about in a more open environment with the Five Eyes.

If we could do that now with NATO, which best I can determine we're on the path to do, that's almost 95 percent of the traffic on the wired side in the world when you put the Five Eyes together with NATO. So I mean if we can come to some common standards on an international basis to talk about these issues about being attacked, describing those attacks, understanding what your standard rules of engagement would be on a military side, understanding what declaratory policy and judicial policy would look like in those environments, and what's appropriate and come to an agreement internationally. Is it just to the first server and stop it? Is it to follow it back or do you wait and do you go through the forensics through a more formal notice through the FBI, say, with that country?

Those are all things that we're starting to do informally but now need some structure around them. I think people are starting to understand this now, but the question is how do you put structure in it, and how do you put structure in it in such a way because any time you put structure to something, there's a down side to it. You're giving something up.

And so that debate needs to be more public, and it needs to go beyond our borders, but we have a particular problem right now with the Chinese, and it's more associated on the national security side, and I think that dialogue has got to occur country-to-country. I've been a party to two sessions with my

counterparts to have this discussion, but quite frankly, the Chinese military is not really where you want to have this dialogue.

You want to have this dialogue as a government-to-government activity, not as a military-to-military activity. The mil-to-mil will come, and it's important, but not as important as coming to an understanding.

I think those are kind of the key issues that I would highlight, and then I'm willing to follow you anyplace on questions.

If I could just say a few words on the nuclear side.

HEARING CO-CHAIR FIEDLER: Please.

GENERAL CARTWRIGHT: Again, my worry, particularly, as we as a government start to disengage, and be careful with that word, but start to move out of Iraq and move out of Afghanistan, and start to reposition ourselves in the world, whether we call it a pivot or whatever we want to call it, the reality here is we've always been in the Pacific. We're going back to the Pacific through the forces that we removed from that venue in order to work in Afghanistan and Iraq to a large extent.

But what should that posture look like? What we clearly are doing is trying to find a way to have a southern hub in the Pacific because we've always had the northern hub. We're worried about the North Koreans. But the southern hub has been an area that we don't have the basing rights. We moved out of our time in Taiwan. We've moved out of our basing in the Philippines. Now, permanent basing in the South Pacific is a problem.

For me, Australia doesn't count in that construct. It's too far south. It's too far away. It is okay to use as a training base and whatnot, but it should not be considered an operational activity.

How are we going to do that? Whether it's a lily pad construct where we kind of move from place to place as we're welcomed. As you watch the tensions rise in the Pacific, we gain more friends here, quite frankly. We've got to be careful about those friends, and we've got to be careful about demonizing China as we do this.

The intent here is not to enter into conflict. The intent is to have stability and ensure the Straits of Malacca and areas like that remain open and that the constructs that we have on an international side remain understood.

So extended boundaries into the sea to get mineral rights and energy rights, et cetera, are problematic for us. Passage through those areas is cut off and costs companies large amounts of money to go around them. Those are things we've got to worry about and that we should be considering about.

So on the strategic side, as you move forward here, they are developing a nuclear capability. It is there. It is not something they need to invent, but the scale of it is the issue here, and we are in this mind-set right now of a pure bilateral relationship with the Russians. They remain the potent arsenal

out there. I understand that. But the reality here is our trade, our activities, our relationships are so interdependent and intertwined with the Chinese that we need to have this dialogue.

What worries me probably the most are the disconnects that tend to occur between their government and their military. You can use the ASAT test. You can use the stealth fighter flight while the Secretary was there. I mean any number of things that point to a disconnect in command and control between the civilian leadership and the military.

They have a different concept than we do of how civil-military comes together, but at the end of the day, we need our senior leaders on the civilian side to be able to have a good relationship, a transparent relationship. We need as a nation to stop thinking bilaterally and now start to think multilateral when we think about nuclear weapons because the activities associated with China and how much it's going to grow, as you watch Russia and the United States start to draw their arsenals down, where do we want to end up in this?

What's the goal? What does it look like? Many of our weapons are associated with first strike type activities or decapitating strike activities. There's a way to negotiate those activities. If we could do that with the Russians, we could drastically reduce the arsenals we have. Do we want to let the Chinese get beyond that and then have to negotiate back? Where do we want to be?

The longer we wait on this thing, the longer we put this off, the more problematic it's going to be for us to have a multilateral approach to nuclear weapons. And that's not just the ability to strike with those, but proliferation and nonproliferation. All of those venues need to be discussed.

It's not that they're not willing, but how do we start to get this into a more authoritative activity so that we can actually start to work in this environment as we move forward? I think this is very critical to how we go forward.

So I'll hold there and open for questions in any of those areas or any place you'd like to go.

QUESTIONS AND ANSWERS

HEARING CO-CHAIR FIEDLER: Thank you very much, General.

We do have a number of questions. I have a quick one. You said that we've never had a nation state refuse to help us when we've singled out a server. Does that include the Chinese?

GENERAL CARTWRIGHT: I cannot comment on specific countries. The challenge--

HEARING CO-CHAIR FIEDLER: Is attribution.

GENERAL CARTWRIGHT: --on many of these is getting back to that server and actually finding it. There are fingerprints--

HEARING CO-CHAIR FIEDLER: Right.

GENERAL CARTWRIGHT: --with any of these attacks, and many of these attacks may have one country's fingerprints but be emanating from another, and so you're going to have to do forensics to some extent to start to follow the path back, but if you find the server that's offending, getting at that server first, to me, is the logical step, whatever country it's in, and then you work on the forensics after that.

HEARING CO-CHAIR FIEDLER: Right. Mike.

COMMISSIONER WESSEL: Thank you for being here and for your earlier testimony and the visit we had, and I'd like to refer back. As Commissioner Fiedler had talked about, last time you were here, you had talked about being--cyber being the WMD of the future.

You mentioned at the front end of your testimony questions about the equipment and the supply chain, and I wanted to get your thoughts. As there is more globalization of the supply chain, and there have been increasing concerns about certain vendors that have at times talked about mitigation steps, et cetera, how do you view that?

Are there ways of taking full mitigation that you can develop confidence in foreign vendors or is there always going to be a certain amount of risk that we have to accept, and the question is what is the tipping point for that confidence?

GENERAL CARTWRIGHT: Yeah. I think that, you know, during my time, at least, in government, we probably went too far in one direction of believing that in many cases, for critical components, we were going to have U.S.-only foundries, so to speak. That's really unrealistic. The systems are too interconnected. It doesn't mean that we shouldn't be wary, we shouldn't have safeguards in place, testing, things like that, but the reality here is that it will drive the cost in such a way that many American companies oftentimes won't be able to compete.

Many of these vendors for things like SCADA systems and other types

of switches are so leveraging in costs to go offshore that it's very difficult to keep your supply chain pure.

Air gapping something, so let's just say it's a special system, and you don't want it connected to anything, well, the first thing you find out is that it almost is connected, always touches something. If it didn't get designed that way, some ingenious young person, old person, whatever, will find a way to get it connected because they'll be trying to help somebody.

Oh, you'd like to have the weather at the same time, here, let me just connect this up for you. You know, if you're in the intelligence community, they're your best allies, and over time somebody is going to penetrate that network. You didn't intend it.

So the idea that the supply chain somehow could be pure in that network is also pretty remote because things break and bosses want things fixed right away so you'll go get what you can get, and oftentimes you don't know the pedigree of that equipment.

So having that, understanding that, is one side of this equation. Having testing, that's important. My sense is there ought to be some sort of testing here, and there ought to be some sort of certification that goes with it so you have a reasonable understanding of the risks that you're taking in your network, understanding that it's going to be connected to a network that's highly risky. Dot-com is still the wild, wild West.

But as you look at this, we need to take mitigation strategies. From a person who has spent the last several years on the offensive side of cyber, one of our best defenses is probably a flaw for us, but there is no such thing as a blueprint that is accurate. There isn't. And there are switches put in and out, and as soon as you change a system, it's very difficult to attack it.

You've now got to go back in. So we tend to be our best, our own best defense. We're also our own worst enemy in that we tend to be sloppy. But the constant changing in our networks, there's no two systems in the electric grid that are exactly the same. None of them are purely to blueprint.

So having the blueprints is an advantage, but it's not necessarily the answer. This is a very difficult activity. This is not television where some 18-year-old will come in and do it. This takes a lot of work and a lot of people to do.

So the question from the supply side from my standpoint is you need to start developing strategies, strategies that change your configuration on a regular basis, strategies that match configurations with other systems to say are they both telling me the same thing? So having duplicate systems, back-up systems, so that you know when you're being deceived, or that you find out as early as possible in the game.

The military has got to get into this, too, and you cannot rely on a single set of sensors, weapons and command and control in the future. It's just

not reasonable. You're going to have to compare multiple sensors against multiple command and control nodes against multiple delivery systems.

If you don't do that, you won't know when you're being lied to. I mean because I can make your display tell you whatever you want to see. So, you know, these are the kinds of things that we have to start thinking. What are the cyber strategies? How do you understand this? But this environment is so leveraging to business and so leveraging to defense, it's a risk-gain activity that you go through.

Nothing is without risk, you know, and you got to look at the gains that you get for it and decide how much risk you're willing to take, and then obviously be prudent and understanding of the risk that you are taking so that when you undertake an activity, you're well aware of the risks that are there, too.

I mean it's just like me going to my bank online. I'm willing to sign up for a reduction in my privacy for higher assurance that the transactions are, in fact, going to happen, and that they'll be cared for, and that they won't be lost or compromised when they occur.

This idea of voluntariness has to be there, but you're going to make a risk-gain calculus each time you do it.

HEARING CO-CHAIR FIEDLER: Thank you.

One more. Dan.

COMMISSIONER BLUMENTHAL: Yes.

HEARING CO-CHAIR FIEDLER: There are actually maybe two more.

COMMISSIONER BLUMENTHAL: Thank you for your testimony.

I had a question regarding taking the point that it shouldn't just be a military-to-military dialogue. In my opinion, just following on this, the greatest risk is obviously a major, a major cyber attack, actually that the Chinese are quite open in writing about and speaking about, and not only on the sort of force-enabling side in terms of what they might do in a conflict scenario, but actually using cyber as a strategic offensive weapon like other countries have already done.

And I just, if you could walk me through the--and I understand part of the problem with the PLA is they just won't talk. I mean that's one of the reasons we need the whole government approach is the PLA doesn't like to talk to us very much.

So if you could walk me through this sort of deterrence thinking on this. I mean it is just so hard to get your head around. I mean, you know, how do you deter a major, you know, a major cyber attack that is not physical in nature, but can still, as you said years ago, bring down a banking system and an electric grid, or that's the next type of thing that might be used against us? Walk me through the early stages of how to think about deterrence.

GENERAL CARTWRIGHT: My sense is that the 21st century deterrence,

whether it be nuclear, whether it be bio, whether it be cyber, is going to, to a large extent, be about anonymity and about attribution. Whether nuclear--you know, it's much more effective, rather than 300 ICBMs coming over the Pole, to take a pick-up truck and park it in the city. Okay.

In bio, it's going to take us a long time to understand where the attack came from. In cyber, it's going to be much the same. Okay. So when you have threats like that, the general deterrent construct is to remove as much as possible the objective from your adversary. So passive defenses talk about, in the kinetic sense, talk about hardening, stand-off distances for terrorists so that vehicles can't get close to buildings, things like this.

You have to think about the same things in cyber. What are the things that you can do that would mitigate the likelihood that a cyber attack could, in fact, drop the whole electrical grid or a banking system or something like that? These are the types of deterrent strategies that you have to think about.

Offense and mutual assured destruction is relatively low in utility in these types of environments. Okay. So you're thinking more about the types of defenses that deny your adversary their objective, and when you think about that in cyber, as I just talked about, it's having back-up systems, it's having good hygiene, which is generally our biggest problem, and I've talked before publicly about there needs to be some sort of public-private organization--I used as an example the FDIC--where you get the stamp on the outside that says I have good hygiene, I've looked at my hardware, I do these kinds of inspections. You can shop here or you can shop there, you know. It's your choice.

But have some sort of a venue like we do with the FDIC that is not pure government, but has the authority to lay down a standard against which you can use.

In the deterrence construct, I go back to the period of the '70s, '60s, '70s, '80s, where we were worried about hijacking in this country, and with a few air marshals, a very low percentage in comparison to the number of flights, the likelihood that you were going to be successful went down sufficiently that the hijackers went away.

You're never going to make it go away completely, but what you're looking for is the knee in the curve. What does it take to make your adversary believe that the likelihood of success has been significantly diminished? That applies all the way up to full-blown war.

Now, I don't believe anybody is going to invade the United States. But for us, I think at least for the next five to ten years, the biggest threat that we have is the unknown. It doesn't take all the banking system to come down. One bank and somebody claiming they cyber hacked it is enough to make you question whether you should go back to the bank tomorrow.

It's the same with an airline or any other thing. So it's less the

massive attack that you worry about; it's the loss of confidence in the country that can occur from a limited attack that is very difficult to put attribution to. Those are the kinds of things I think that we have to worry about.

COMMISSIONER BLUMENTHAL: If you would, explain why the retaliatory strategy would not work?

GENERAL CARTWRIGHT: Well, number one, it's not immediate and proximate.

COMMISSIONER BLUMENTHAL: Okay.

GENERAL CARTWRIGHT: I mean that's the biggest problem.

HEARING CO-CHAIR FIEDLER: Time for one last question. Larry Wortzel.

HEARING CO-CHAIR WORTZEL: General, thank you very much for thoughtful testimony and for agreeing to come out here a second time.

I want to take you back to your days as the STRATCOM commander and talk about nuclear issues. The Russians have changed much of their warfighting doctrine, particularly in the Far East, and are reintroducing tactical and even what boils down to nuclear weapons because of their lack of manpower and weakness.

It seems to me that makes the fire break between conventional and nuclear war more fragile and makes nuclear war more likely. Is China likely to mirror that Russian doctrine in self-defense, and if they do, what does that do to INF forces and treaty?

GENERAL CARTWRIGHT: I think there's a couple of axioms that still seem to hold true. Nation states acquire nuclear weapons as a shield. Terrorists acquire them as a weapon, as a sword. That tends to still be true.

Nations that believe that the strength of countries that might, in fact, pose them threat, when that strength is substantial and outnumbers in significant ways, whether it be in weapons or people, nuclear weapons become a leveler--okay--in their mind.

Russian military is not growing. It's decreasing, and you can look at the demographics of the country. They're on the decline from a pure who could be in the military standpoint. The number of systems they have are declining. When they look to their south, they see nothing but growth, and they see nothing but large numbers.

So for the Chinese, it doesn't make a lot of sense to go that path, but for the Russians, they're starting to perceive a threat. They may believe there is still a threat from Europe. To us it doesn't make sense, but that's their own psyche.

So they're looking at threats that they can no longer outman. They certainly can out-quality in many venues, but the numbers game is working against them, and they look at these things as being right on their borders, not across the ocean from them or something like that, and so they're very proximate

threats.

As you start to look at treaty constructs, as we go forward, we certainly need to be mindful of that threat and their perception of that threat. It's very real to them. Okay. We can't just dismiss it with why can't you just agree to get along?

And so as we go beyond new START, we need to now start to understand the implications of cyber, missile defense, long-range conventional, and then nuclear. And we probably need to start to find a way to get away from just a pure us versus Russia long-range strategic weapons and get into a more fulsome dialogue, but doing that in the silos of tactical, strategic, conventional is not going to do us well.

We've got to start to make the problem harder to understand the context in which we're making these decisions because doing it in the Aegis is not working for us. Just taking care of long range strategic makes us feel good, but it isn't solving the global problem.

HEARING CO-CHAIR WORTZEL: Thank you very much.

HEARING CO-CHAIR FIEDLER: Thank you very much, General. Always good to see you again.

GENERAL CARTWRIGHT: Thank you. Take care.

HEARING CO-CHAIR FIEDLER: Thank you.

The next panel--just a couple of minutes while the next panel assembles.

[Pause.]

PANEL I – CYBERSECURITY

HEARING CO-CHAIR FIEDLER: Okay.

HEARING CO-CHAIR WORTZEL: All right. Please take your seats. We're going to start the first panel of the day.

Our first panel is on cyber issues, and we're pleased to welcome three of the best in the field: Richard Bejtlich, Nart Villeneuve--did I get that right?

MR. VILLENEUVE: Yes.

HEARING CO-CHAIR WORTZEL: Thank you. And Jason Healey.

Mr. Bejtlich is Chief Technology Officer at Mandiant. He's a former military intelligence officer and has over 13 years experience in enterprise level intrusion detection and incident response. He's authored several books on the subject and reviewed dozens of books.

Mr. Villeneuve is a senior threat researcher at Trend Micro where he focuses on targeted malware attacks, botnets, and the criminal underground.

Previously, his technical research at the University of Toronto led to the discovery of two cyber espionage networks, GhostNet and ShadowNet-- and there were two great publications on that--which compromised foreign governments and missions.

Mr. Healey is the Director of the Cyber Statecraft Initiative of the Atlantic Council, focusing on international cooperation, competition and conflict in cyberspace. He's got extensive experience in the private sector and the White House and began his career in the U.S. Air Force.

Thank you for being here. A couple of procedural notes. We expect Representative Wolf around 11 a.m., and we're going to just hold the panel and yield for his remarks.

Second, I want to remind you that we try and hold the testimony itself to seven minutes, which we have your written statements, and we've read them, but it leaves a lot more time for questions. You saw we didn't have much time for questions before.

So, Mr. Bejtlich, we'll let you begin. Thank you.

OPENING STATEMENT OF RICHARD BEJTLICH
CHIEF SECURITY OFFICE, MANDIANT

MR. BEJTLICH: Good morning, Mr. Chairman, members of the committee, and thank you for the opportunity to contribute to today's hearing.

I'm the Chief Security Officer at Mandiant, and if I could be the CTO, that would probably be a nice promotion, but for now I'm the Chief Security Officer.

We're a private company that provides software and services to detect and respond to digital intrusions. My testimony draws on our company's experience as well as four years defending General Electric as Director of Incident Response, and I've defended Western interests against serious intruders since 1998 when I was a captain in the Air Force.

Because my most recent experience draws on work done in the private sector, I'm not the person to ask about the structure of the Chinese military or the actual roots that are behind it. However, I can give you my company and my colleagues' perspectives on this problem.

Our intelligence team tracks about 20 groups that we designate as Advanced Persistent Threat actors. We tend to take the strict definition of APT, as defined by the Air Force in 2006, as groups that are acting from China.

We currently categorize these groups as having different skill levels. We categorize about a quarter of those 20 to have what we would consider high skill, about one-quarter having medium skill, and, as you might expect, one-quarter having low skill. The final quarter are groups that we have just recently identified, and we don't have enough data yet to tell you whether you consider them high, medium or low.

Most of the groups we track target the U.S. defense industrial base, but also some of these groups target U.S. government agencies, think tanks, political organizations, and other commercial and private targets, and our most recent report broke out the percentages of activity against different elements of this nation's infrastructure.

So 23 percent of the activity that we saw covered communications companies, and by that I don't mean ISPs, I mean people who make telecom gear; 18 percent affected aerospace and defense; 14 percent computer hardware and software; ten percent energy or oil and gas; ten percent electronics; and the remaining quarter was considered "other," of which the financial sector was the largest.

You'll notice if you compare those sorts of companies and industries to your last year's report, it matches up pretty nicely with some of the strategic sectors that China has targeted.

I have a couple of case studies where I'd like to illustrate some trends

we've seen in intrusions linked to China. The first case describes APT actors who assembled intellectual property that they needed to replicate a product, and the second one describes APT actors who are present during merger and acquisition activities.

In the first case, in early 2011, and these are all from just last year for your reference, we were contacted by an electronic components manufacturer as a result of a notification by a third-party, namely, a government agency.

We discovered that this organization had had technology stolen from it, and the victim did not place a lot of value on that particular component because what they said was this component is something that you have to pair with another piece of technology in order to have value. Now, clearly, they were making it; they were selling it. But they said I don't understand why an intruder would want this; you have to put it with something else.

Well, wouldn't you know two weeks later, we got a call from that second company that made the other half of the component, and they said somebody just stole this from us. We don't understand what the deal is, but we don't think it has that much value because you need Part A. Well, we were in a position to see Parts A and B stolen, put them together, and obviously the intruders had the same sort of interest as well.

The second case involved a large European defense contractor. They also had received a third-party notification that there was a problem. They suffered the same sorts of intrusions as you probably read in the news, malicious PDF attachment, user clicks on it, the intruder then proliferates throughout the environment. In the course of our investigation, we found that the intruder had ultimately stolen about 50,000 files, and the thing that was interesting about this case was that this large organization was in the course of doing merger and acquisition activities.

Specifically, they were looking at buying a smaller company, and what we found was that this smaller company was completely compromised by Chinese actors, and so as a result of our work with both these organizations, we were able to find the problem, take care of it, and then move on.

This idea of the Chinese going after smaller organizations that have been identified as being about to be acquired by larger ones seems to be a trend because a lot of the companies that you see represented in the audience today, they've done a good job hardening themselves against these bad guys, but the smaller ones aren't there yet.

I've got a couple other statistics I'd like to share based on our analysis of these groups over the last year. 94 percent of our victims learn of the compromise via third party. That's mostly the FBI. There is some NCIX and some by some other means. That means only six percent found it themselves. Most of these organizations just don't have the tools, processes, staffs, or mind-set

necessary to deal with these intruders.

Secondly, the median number of days that elapsed between where we found the intruder getting into a company and someone doing something about it was 416. In other words, these intruders are in these organizations well over a year, doing whatever they want before anyone even notices.

The only bright side to this is this is actually a decrease. Typically it's two to three years, and you have even seen the public Nortel case where it was something on the order of ten years.

And, then, finally, we have seen the bad guys using stolen credentials in 100 percent of the cases. So whenever you focus on tools, you're going to miss a lot of the cases because the bad guys are going in there stealing credentials and then look like normal users.

Now, it's important to realize these groups use the level of sophistication they need to accomplish their objective, but I prefer to emphasize the advanced nature of the intrusion management skills when explaining that these groups, you've got some of the most motivated, well-resourced, well-staffed companies in the world fighting these guys, and no one has solved this problem. And so it really speaks to more of a larger picture than what we have here.

Finally, Mandiant is not aware of any specific attacks against an organization's supply chain or cloud infrastructure. Supply chain attacks can be detected, but to tell you the truth, the cloud attacks really worry us because it is difficult for a cloud victim to know that something has happened, and it's difficult for the cloud provider to tell that something has happened.

You want to talk about the Internet being the "Wild West." The cloud is certainly a Wild West out there.

And finally, two recommendations that I would make. First, I recommend Congress consider an "are you compromised" assessment to be done on an annual basis to tell if organizations have been compromised, as opposed to something like an "are you vulnerable," because everyone is vulnerable.

And then, secondly, I recommend the adoption of an open standard for exchanging technical data. Our company has something called OpenIOC that would help in this regard.

I thank you for the opportunity to testify, and I welcome your questions.

PREPARED STATEMENT OF RICHARD BEJTLICH
CHIEF SECURITY OFFICE, MANDIANT

March 26, 2012

Richard Bejtlich

Chief Security Officer, Mandiant

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on "Developments in China's Cyber and Nuclear Capabilities"

Mr. Chairman, members of the Committee, thank you for the opportunity to contribute to today's hearing. I am Chief Security Officer at Mandiant, a private company that provides software and services to detect and respond to digital intrusions. My testimony draws on our company's experience, as well as four years defending General Electric as Director of Incident Response. I have defended Western interests against serious intruders since 1998 when I worked as an analyst and intelligence officer at the Air Force Computer Emergency Response Team, the Air Force Information Warfare Center, and the Air Intelligence Agency.

Because my most recent experience relies on work done in the private sector and enterprise customers, I am not able to provide first-hand answers to questions concerning China's military, security services, criminal groups, or other parties. Your recently released reported titled "Occupying the Information High Ground" is a better source of information on specific, named organizations within China, such as the People's Liberation Army's Third and Fourth Departments of the General Staff Department.

However, I can comment on the characteristics of the groups that the Mandiant Intelligence Team has identified as Advanced Persistent Threat, or APT, actors. For the most part, our team and I use the strict definition of APT as created by the Air Force in 2006, namely as an unclassified reference to intrusions sets ultimately traced back to actors in China. Members of our team have extensive knowledge of these actors that includes time at Mandiant and other organizations focused on the threat from the Asia-Pacific region. Mandiant's assessment of APT actors is not based on any single aspect of an intrusion, such as an IP address owned by a Chinese registrant, or the presence of Chinese language characters in malicious tools or other code. Rather, Mandiant dynamically tracks, over time and subject to continuous modification and refinement, APT groups using a variety of indicators of compromise.

Our intelligence team currently tracks approximately twenty distinct APT groups. These groups include all of the parties identified by reports publicly released by other security companies, as well as actors

that we believe are unknown to many of those other companies. We have seen these groups demonstrate various levels of technical and organization skill, with approximately a quarter having "high" skills, one quarter having "medium" skills, one quarter having "low" skill, and one quarter too new to make a characterization. Within APT groups we tend to see evidence of "crews," meaning smaller teams who specialize in various stages of a compromise. For example, one crew may be tasked with obtaining access to the victim; a second crew moves laterally through the organization to gather intellectual property or other data; and a third crew steals or exfiltrates the data.

Most of the APT groups we track target the US defense industrial base (DIB). Some of these groups also target US government agencies, think tanks and political organizations, and other commercial or private targets. Our most recent M-Trends research report described our consulting caseload for 2011 in these terms:

- Communications companies: 23%
- Aerospace and defense: 18%
- Computer hardware and software: 14%
- Energy or Oil and Gas: 10%
- Electronics: 10%
- Other, of which the financial sector was the largest component: 25%

The following case studies illustrate the trends we have seen in computer intrusions linked to China. The first case describes APT actors assembling the intellectual property they need to replicate a complete product. The second case describes APT actors present during merger and acquisition activities.

In early 2011, an electronics component manufacturer contacted Mandiant as the result of receiving a notification of compromise from a government agency. After conducting sweeps to obtain forensic evidence, we realized that the attacker had been replacing their malware every six months during the two years they had been resident at the victim organization — and this replacement occurred again during the course of our investigation.

To maintain persistence, the attacker used a variety of backdoors, including some publically available ones. One interesting custom backdoor consisted of a custom miniport driver, which listened for a particular "magic packet" that, when received, would activate the malware. Of the approximately 100 compromised systems at this customer, the intruder installed malware on less than half of them. For access to the other systems, the intruder relied on usernames and passwords stolen from the organization.

Mandiant consultants were able to forensically recover a partial listing of stolen intellectual property. The victim company did not place a high value on the stolen data since it was merely a sub-component

of a more advanced technology, and the victim did not even produce the other component parts. While the more advanced product was extremely valuable, it could only be built by combining the victim's technology with parts from a second company in the supply chain. Within weeks, however, the second company called Mandiant. They had also been the victim of an advanced attack, and they also lost intellectual property for a sub-component. It was only by connecting the dots between the two victims that the attacker's goal was clear: rather than targeting a single company for a particular technology, they had been tasked to acquire the more advanced, broader technology. The attackers had performed reconnaissance to determine what companies produced the component technologies, and then targeted those entities to steal what they needed.

Later in 2011, a large European defense contractor contacted Mandiant just months after acquiring a specialty service provider. The service provider had received information indicating that they had been the victim of a targeted attack, and the parent company was concerned about the extent of the penetration.

The attack began with a phishing email containing a malicious PDF attachment. Prior to sending the email, the attacker had performed enough reconnaissance to uncover the name of an individual at a competing organization with whom the victim user had previously corresponded. The socially engineered email purported to be from that individual. When the victim opened the malicious attachment, an intruder established a foothold in the environment. The attacker leveraged this initial backdoor to move laterally throughout the environment, obtained legitimate credentials, and ultimately stole over 50,000 files.

Based on the lessons learned from this incident, the parent company implemented a process requiring every new acquisition to be vetted by the Mandiant Intelligent Response tool prior to being allowed to join the corporate network. This process paid off in late 2011 when the company discovered an APT group actively operating at another company they were about to acquire. The integration was put on hold until a thorough remediation and damage assessment was completed.

Through these sorts of cases, Mandiant extracted several other statistics which describe trends seen in computer intrusions attributed to APT groups.

- 94% of victims learn of compromise via third parties; only 6% discover intrusions independently. Victim organizations do not possess the tools, processes, staff, or mindset necessary to detect and respond to advanced intruders.
- The median number of days that elapse between compromise of a victim organization and detection or Mandiant involvement is 416 days. Incredibly, this number is an improvement over past intruder "dwell time" measurements of two to three years.
- Advanced intruders installed malware on 54% of systems compromised during an incident. They did not use malware to access the other 46% of systems compromised during an incident, meaning relying on tools that find malicious software misses about half of all victim computers.

- Mandiant observed intruders using stolen credentials in 100% of the cases it worked in 2011. Intruders seek to use legitimate credentials and access methods as soon as possible, because they can then "blend in" with normal user activity.

APT groups use the level of sophistication required to achieve their objective. For example, in 2011 Mandiant observed an increase in the usage of publicly available malicious tools by APT actors. We assess that the adversary uses publicly available tools for three reasons:

1. They already exist, so the intruder does not need to expend research and development resources to create custom tools.
2. Many organizations allow internal use of the sorts of tools favored by intruders.
3. Publicly available tools rarely stand out against the "noise" created by lower-level intruders pursuing smash-and-grab or "botnet" intrusions.

The use of public tools or leveraging publicly known vulnerabilities is a source of confusion for many security professionals. They assume the "advanced" element of the APT term requires that Chinese actors deploy the most sophisticated digital weapons for all phases of an intrusion. I have personally observed APT actors escalating their technical sophistication to adapt to countermeasures deployed by computer incident response teams, so I know the APT can be as advanced as needed when the target warrants it.

I prefer to emphasize the advanced nature of Chinese intrusion management skills when explaining the sophistication of APT groups. It is significant that the most well-resourced, highly professional, and motivated network defenders on the planet have not yet "solved" the problem of Chinese intrusion activity. At best we can keep them from stealing the bulk of an organization's crown jewels, but only after significant investment in improved technology, business and IT processes, partnerships, and staffing.

Mandiant is not aware of specific attacks against an organization's supply chain or cloud infrastructure in order to steal intellectual property, beyond what has been publicly mentioned in the press. Attacks against the supply chain, when manifested as malicious code in trusted hardware or software, can sometimes be discovered by end user organizations. Local security staff can identify the malicious code by the action it takes on the network, or by the way an adversary interacts with it. It is difficult for end user organizations, and any consultants they hire, to gain visibility and awareness concerning compromise of cloud platforms. In general, do not expect cloud providers to be able to identify adversary activity, because it is difficult for the cloud provider to differentiate between legitimate and illegitimate access and use.

APT groups continue to focus on enterprise Windows computers, although other operating systems have been compromised. Intruders exploit enterprise systems hosted in company-owned data centers,

and enterprise systems hosted at third party data centers. For the most part, mobile devices, true "cloud infrastructure," and tablet computers do not yet appear to have been targeted.

Concerning legislative or administrative actions that the U.S. Congress can take, I have two recommendations. First, I believe far too much legislative and regulatory attention is paid to compliance with standards and the question of "are we vulnerable?" In my professional opinion, compliance with standards is, at best, effective at stopping some lower-skilled intruders who opportunistically exploit targets. Compliance regimes tend to devolve into a paperwork exercise based on subjective interpretations and the whims of an auditor.

Regarding the question of "are we vulnerable," the answer for every organization is "yes." Rather than wasting time on this question, organizations should instead ask themselves "are we compromised?" In other words, does the organization suffer an ongoing intrusion by a targeted intruder, whether from China, Russia or a criminal group? It is a waste of time and resources seeking compliance with standards while intruders are actively stealing data from a victim organization. The adversary will adapt to any countermeasures deployed during the compliance exercise; I have seen this pattern repeated regularly during my career.

To this end, I recommend Congress consider the integration of an "are you compromised" assessment into any new requirements levied on specific industries. These assessments should occur no less frequently than once per year, although true continuous assessment on a 30-day cycle is much more effective in my professional judgement and experience. By requiring processes and technology to answer the "are you compromised" question, regulators, Congress, and other appropriate parties will, for the first time, gather ground-truth knowledge on the state of security in selected industries. Without knowing the real "score of the game," it is unreasonable to expect real progress in digital security.

My second recommendation involves sharing threat intelligence. I offer a few principles based on my experience as someone who has created, consumed, and shared threat intelligence in a variety of public and private roles.

1. First, adopt an open standard for exchanging technical data. Mandiant created the Open Indicator of Compromise, or OpenIOC format (http://www.openioc.com) for this very purpose. It allows fine-grained description of threat intelligence for use by analysts and software and is free of charge with an open specification available online.
2. Second, recognize that dozens of effective threat intelligence sharing organizations already exist. These include the Defense Industrial Base Collaborative Information Sharing Environment (DCISE), the Bay Area CISO Council, the Financial Services Information Sharing and Analysis Center (FS-ISAC), as well as other ISACs, and other groups. Understanding and coordinating efforts among these groups is a good precursor to any additional sharing activity.

3. Third, please note that intelligence sharing networks do not necessarily improve as additional members join. Having participated in these networks, I have seen a tendency for participants to guard their contributions as the network adds those for whom trust cannot be established on an interpersonal basis. Intelligence sharing relies on trust in order to succeed, and trust is built on personal relationships.

Thank you again for the opportunity to testify. I welcome your questions and comments.

HEARING CO-CHAIR FIEDLER: Thank you very much.
HEARING CO-CHAIR WORTZEL: Mr. Villeneuve.

OPENING STATEMENT OF NART VILLENEUVE
SENIOR THREAT RESEARCHER, TREND MICRO

MR. VILLENEUVE: I would like to thank the members of the Commission for inviting me today.

I spend most of my days investigating targeted malware attacks at Trend Micro. My statement today is drawn from my experience in the two cases that you mentioned, GhostNet and ShadowNet, but also a third report that I put out recently called LURID, which demonstrated that the same threat actors that were attacking interests in the United States have shifted focus and have started targeting space-related agencies in Russia and the former Soviet Union.

My statement is entirely my own opinion and does not necessarily reflect the views of my employer.

I prefer to call these targeted malware attacks, whereas others prefer to see them as a component of or directly call them Advanced Persistent Threat activity. I believe that this activity can be tracked over time and linked through specific indicators to threat actors operating in the Chinese language or using command and control infrastructure based in China or operating command and control infrastructure from China.

However, I recommend caution when attempting to determine attribution based solely on technical indicators that are frequently spoofed and often misleading. As the General mentioned this morning, I don't believe there's a "smoking gun" in cyberspace.

While there have been a lot of accusations of hype surrounding several highly publicized attacks, the problem of targeted malware attacks is severely understated, not overstated. Instead of focusing on the effect of these attacks, most seem concerned with the level of sophistication and debate whether these attacks are advanced or not from a technical perspective.

So I would like to emphasize three points:

First, targeted malware attacks are extremely successful. The scope of the problem is truly global, extending far beyond the U.S. It affects governments, militaries, defense industries, high-tech companies, the energy and finance sectors, intergovernmental organizations, nongovernmental organizations, media outlets, academic institutions and activists around the world.

Often these attacks target communities of interest that span these categories. And once a compromised soft target is available, they can use that to

launch attacks on more hardened targets. And these attacks are successful because they leverage social engineering, or the art of manipulation, in order to trick individuals into revealing sensitive information or executing malicious code.

The second point I want to make is that these targeted malware attacks are not isolated incidents of "smash and grab." We tend to see a lot of focus around particular events, but I believe that it's better characterized as malware-based espionage, or consistent campaigns that are a series of failed and successful attacks against targets over time. And the objective is to establish a persistent covert presence in a target's network so that information can be extracted as needed.

They don't necessarily need to grab something right away, but they want to be able to obtain the information they want when they want it.

And one of the most important and often overlooked elements of these campaigns is the reliance on human labor, which stands in stark contrast to the largely automated botnets operated by cyber criminals.

In addition to manual reconnaissance, the attackers will craft individualized e-mails and package malware specifically for an individual group or a group of targets. In addition, they'll adjust their tactics in reaction to the defenses of the victim.

One of the trends I'm seeing is a lot of malware groups that have been used in the past heavily in North America are now shifting focus, focusing on former Soviet Union, Taiwan, Japan, and Vietnam, as well.

This customization and low level of distribution provides the attackers with a significant advantage over defenders that are largely relying on automated systems.

Third, targeted malware attacks are not well understood. However, careful monitoring and investigation can leverage mistakes made by the attackers that allow us to get a glimpse inside their operations.

These campaigns can be tracked over time through a combination of technical and contextual indicators, but this information is not often made public.

While some might believe that the threat actors behind these campaigns have mythical capabilities both in terms of their operational security and the exploits and malware tools they use, in fact, they often use older exploits and simple malware. They do not always use "zero day" vulnerabilities, or exploits for vulnerabilities for which there is no patch available.

The objectives of these attacks is to obtain sensitive data. The malware used in the attacks is just an instrument.

So I make the following recommendations:

First, we need to broaden the scope of the stakeholders. While U.S. government, military, critical infrastructure and defense industrial base are well understood as targets and often exchange information amongst each other, the

scope extends globally, and government needs to engage additional stakeholders, both inside and outside the U.S.

Major malware-based espionage campaigns have been uncovered and disclosed by researchers and private companies who need clear avenues for information exchange. One of the problems I've personally faced is who to tell about what I know.

In addition, the NGO community, particularly those involved in democracy promotion, human rights campaigns, as well as Tibetan activism, are also being targeted by the same campaigns we see threatening the national security of the United States.

While many of these threats are understood by a select few, including a lot of people in this room today, the indicators that are so critical to defense are rarely shared outside of trusted circles in order to avoid potentially tipping off the attackers, who may subsequently adapt and change tactics.

However, the scope of the problem is so severe that I recommend broadening stakeholder engagement with diverse communities in order to build a wider network of trust so that the threat intelligence that is so critical to defense can be shared.

Finally, I'd like to encourage responsible disclosure of compromise. No one wants to admit that their organization has been compromised. However, this obscures the problem. It hides the constant attacks and successful penetrations by a discrete set of malware-based espionage campaigns.

When Google broke the disclosure barrier and revealed that they had been breached in what is now known as "Operation Aurora," it firmly placed the issue of targeted malware attacks in the public domain, and they made it clear that companies face the same attacks that had previously focused on government and military networks.

Recently the Securities and Exchange Commission has been encouraging companies to disclose such attacks because they recognize the effect as well as their importance to investors. Ultimately, the public needs to understand the full scope of the cyber espionage problem, and unless incident disclosure occurs, the public will fail to grasp the severity of the situation.

Thank you.

PREPARED STATEMENT OF NART VILLENEUVE
SENIOR THREAT RESEARCHER, TREND MICRO

U.S.-China Economic and Security Review Commission
Hearing on "Developments in China's Cyber and Nuclear Capabilities"
Submission by Nart Villeneuve
March 26, 2012

I would like to thank the members of the U.S.-China Economic and Security Review Commission for inviting me to participate in today's hearing on Developments in China's Cyber and Nuclear Capabilities. I spend my days investigating targeted malware attacks as a Senior Threat Researcher at Trend Micro Inc. While my statement today is drawn from my experience, particularly from an inside view into three cyber-espionage campaigns that I have helped uncover, GhostNet (which compromised diplomatic entities around the world), ShadowNet (which targeted the Indian government and military) and LURID (which targeted space-related agencies in the former Soviet Union), it is entirely my own opinion and does not necessarily reflect the views of my employer.

My testimony today focuses on malware-based espionage, or what some refer to as, or as a component of, Advanced Persistent Threat (APT) activity. This APT activity can be tracked over time and linked through specific indicators to threat actors operating in the Chinese language or using command and control infrastructure in China. However, I recommend caution when attempting to determine attribution based solely on technical indicators that are frequently spoofed and often misleading because there is no "smoking gun" in cyberspace.

While there have been a lot of accusations of "hype" surrounding APT, the problem is severely understated, not overstated. Instead of focusing on the effect of these attacks, most are concerned with the level of "sophistication" and debate whether these attacks are "advanced" or not. I would like to emphasize three key points:

- Targeted malware attacks are extremely successful. The scope of the problem is truly global, extending far beyond the US. It affects governments, militaries, defense industries, high tech companies, the energy and finance sectors, inter-governmental organizations, non-governmental organizations, media outlets, academic institutions, and activists around the world.
- Targeted malware attacks are not isolated incidents of "smash and grab" attacks. They are part of consistent *campaigns* aimed at establishing a persistent, covert presence in a target's network so that information can be extracted as needed.
- Targeted malware attacks are not well understood. However, careful monitoring can leverage mistakes made by the attackers that allow us to get a glimpse inside their operations. Moreover, these malware-based espionage campaigns can be tracked over time through a combination of technical and contextual indicators but this information is not often made public.

1. Targeted Malware Attacks

There has been dramatic increase in targeted malware attacks. Unlike the largely indiscriminate attacks that focus on stealing credit card and banking information associated with cybercrime, these targeted attacks are noticeably different and are better characterized as malware-based espionage. These highly targeted attacks are computer intrusions staged by threat actors that aggressively pursue and compromise specific targets, often leveraging social engineering or the "art of manipulation", in order to maintain a persistent presence within the victim's network so that they can move laterally and extract sensitive information.

In a typical targeted attack, a target receives a message – such as an email or instant message – that is contextually relevant to the potential victim and encourages the target to click on a link or open a file. The links and files sent by the attacker contain malicious code that exploits vulnerabilities in popular software. The payload of these exploits is malware that is silently executed on the target's computer. This exploitation allows the attackers to take control of and obtain data from the compromised computer. The malware connects back to command and control servers under the attacker's control from which the attackers may then command the compromised computer to download additional malware and tools that allow them to move laterally throughout the target's network. These are not isolated incidents of "smash and grab" attacks but are part of consistent campaigns aimed at establishing a covert presence in a target's network so that information can be extracted as needed.

Targeting

While government and military networks have long been targets, these highly targeted attacks have spread to the defense industrial base and high tech companies, the energy and finance sectors, telecommunications companies as well as media outlets, civil society organizations and academic institutions. Often, these attacks target "communities of interest" that span the aforementioned categories. Compromised "soft" targets can then be used to launch attacks against hardened targets. These attacks are successful because they are designed to manipulate individuals into revealing sensitive information or executing malicious code. The delivery mechanism, usually an email, is often specifically addressed to the target and appears to have originated from someone within the target's organization or someone in target's social network. In extremely targeted cases, attackers may actually send email directly from a compromised, but real, email account of someone the target knows and trusts.

While some might believe that the threat actors behind targeted malware attacks have mythical capabilities, both in terms of their operational security and the exploits and malware tools used, they, in fact, often use older exploits and simple malware. They do not always use "zero day" vulnerabilities – exploits for vulnerabilities for which there is no patch available. The objective of these attacks is to obtain sensitive data; the malware used in the attacks is just an instrument. The discovery of GhostNet, for example, highlighted the fact that attackers do not need to be technically "sophisticated" or "advanced". With some functional but less-than-impressive code along with the publicly available gh0st RAT tool these attackers were able to compromise and maintain persistent control of embassies around the world. They can be successful without being "advanced" because of their exploitation of trust through social engineering as well as the learning gained from continual probes as well as both successful and unsuccessful attacks. This allows the attackers to select exploits based on what they know about the target's environment and they do leverage "zeroday" exploits when needed.

Campaigns

These targeted attacks are rarely isolated events; in fact, they are constant. It is more useful to think of them as *campaigns* – a series of failed and successful attempts to compromise a target over a period of time. In fact, the attackers themselves often keep track of the different attacks within a campaign in order to determine which individual attack compromised a specific victim. As the attackers learn more about their targets, from open source research as well previous attacks, the specificity of the attacks may sharply increase.

Once enough information is obtained from separate incidents *indicators* obtained from technical, operational and contextual artifacts can be assembled that allow attacks to be grouped in campaigns. This analysis is important because the information gleaned from any individual incident is usually partial because there are varying levels of visibility across the stages of an attack. For any one incident, we may have the attack vector, such as an email, or the malware payload of simply command and control server activity. Others, especially those involved with incident response, may have information on the attacker's lateral movement and data ex-filtration points. But the most revealing information usually comes from mis-configured command and control servers used by the attackers that reveal an inside look at their operations.

Operations

One of the most important and often overlooked element of malware-based espionage is reliance on human labor which stands in stark contrast to the largely automated botnets operated by cybercriminals. In addition to manual reconnaissance the attacker will craft individualized emails and package malware specifically for an individual or group of targets. In addition, they will adjust their tactics in reaction to the defenses of the victim. This customization and low distribution provides the attackers with a significant advantage over defenders that are largely relying on automated systems. However, this human element also, occasionally, exposes one of their weaknesses.

The attackers can and do make mistakes. Careful monitoring of their command and control infrastructure can reveal the inner workings of their operations. The data obtained from the attacker's infrastructure often reveals the length of the operation, the number of individual attacks, the identity of the victims, additional tools used by the attackers and sometimes even the data that has been ex-filtrated.

The data often reveals the breadth of the victims the attackers are targeting and it is almost always broader than the conventional wisdom based on analysis of individual or even small clusters of activity. While a campaign may maintain subsets of infrastructure for specific geographic regions we have found that campaigns often have a global, thematic focus. While there are often exceptions, the attackers often target "communities of interest" that stretch across geographic boundaries. We have found that campaigns that are well known in the U.S. aggressively targeting Asia (particularly Taiwan, Japan, South Korea and Vietnam) as well as Russia and Central Asian countries.

The information obtained from the attacker's command and control servers reveals that the average length of compromise is considerable. In the case of GhostNet, for example, we found that the average compromise was 145 days with many being compromised for over 400 days (the longest was 660 days). In other cases, such as LURID, we were able to discover the campaign codes the attackers were using which revealed that they had conducted 301 attacks in a two month period (between June 9 2011 and August 3 2011).

The data may reveal the IP addresses from which the attackers are interacting with the command and control servers. In the past, as was the case in GhostNet, the attackers often hosted their infrastructure in China. We now see command and control servers hosted in a variety of countries, especially in the U.S. Furthermore, the attackers are often using tools such as "Htran" that allow them to "proxy" through an intermediary computer so that the attackers and the victims computers never directly connect to one another. These developments further obfuscate attribution.

2. Recommendations

Broaden the scope of stakeholders. While the US government, military, critical infrastructure and defense industrial base are well understood as targets and often share information amongst each other, the scope of the threat extends globally and government needs to engage additional stakeholders both inside and outside the US. Major malware-based espionage campaigns have been uncovered and disclosed by researchers and private companies who need clearer avenues of information exchange. In addition, the NGO community, particularly those involved in democracy promotion and Tibetan activism, are also being targeted by the same campaigns that threaten the national security of the US. While many of these threats are understood by a select few, the indicators that are so critical to defense are rarely shared outside trusted circles in order to avoid potentially tipping off the attackers who may subsequently adapt and change tactics. However, the scope of the problem is so severe that I recommend broadening stakeholder engagement with diverse communities in order to build a wider network of trust so that the threat intelligence that is so critical for an active defense can be shared.

Encourage responsible disclosures of compromise. No one wants to admit that their organization has been compromised. However, this obscures the true extent of the problem. It hides the constant attacks and successful penetrations by a discrete set of targeted malware campaigns affecting governments, businesses and civil society organizations around the world. When Google broke the disclosure barrier and revealed that they had been breached, in what is now known as "Aurora", it firmly placed the issue of targeted malware attacks in the public domain and made it clear that companies face the same attacks that had previously focused on government and military networks. Recently, the SEC has been encouraging companies to disclose cyber attacks because they recognize the effect of such attacks and their importance to investors. Ultimately, the public needs to understand the full scope of the APT problem.

Thank you for the opportunity to testify today on this very important issue. I appreciate the continued good work by the commission and your holding this field hearing here in Manassas. As you know, northern Virginia was really the birthplace of the Internet in the 1980s and 1990s and remains the East

Coast “high tech” hub today.

Today, northern Virginia is one of the frontlines in the emerging cybersecurity challenge, with a significant cyber workforce that is supporting U.S. defense and civilian agencies.

I have been deeply concerned about the cyber threat from China for nearly a decade. When I first started raising these concerns, the general attitude of the U.S. government was to keep everything secret – or in some cases – just to ignore the threat. In fact, when the Chinese attacked four of my office computers in 2006, along with many other House offices and committees, the FBI and others urged me not to disclose it publicly.

After nearly two years of waiting, I took to the House floor in June 2008 to inform my colleagues – and the American people – about the incident and warn of the growing threat to the U.S. government and businesses.

I believed it was important for the public to better understand this threat and what the attackers wanted – not national security secrets, but information about Chinese dissidents with whom I had had worked.

The attacker first hacked into the computer of my foreign policy and human rights staff person, then the computers of my chief of staff, my legislative director, and my judiciary staff person. On these computers was information about all of the casework I have done on behalf of political dissidents and human rights activists around the world.

The computers in the offices of several other Members were similarly compromised, as well as a major committee of the House, the Foreign Affairs Committee.

It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress to help people who are suffering around the world was also open to view from these official computers.

In subsequent meetings with FBI officials, it was revealed that the outside sources responsible for this attack came from within the People's Republic of China. These cyber attacks permitted the source to probe our computers to evaluate our system’s defenses and to view and copy information. My suspicion is that I was targeted by Chinese sources because of my long history of speaking out about the Chinese government’s abysmal human rights record.

I have spent hours with countless Chinese dissidents ranging from Uyghur Muslim activist Rebiya Kadeer, to house church pastor and advocate Bob Fu, to former laogai prisoner Harry Wu.

Just recently I visited with an impressive group of Chinese lawyers in Washington for the National Prayer Breakfast. To a person, each loved their country and where rightly proud of their heritage. But all sought fundamental change. They longed to live in a land where they could worship freely, speak openly and enjoy the basic protections of a constitution grounded in rule of law. Their quarrel – and mine – is with a thin layer of leadership at the helm of the Chinese communist party that rules by fear

and oppression.

Since I spoke out in 2008, there has been a "sea change" in how senior defense and intelligence officials are publicly discussing to the cyber threat. Four years ago, some of these same leaders who were warning against even publicly acknowledging cyber attacks – much less the source of the threat – are now publicly warning of the threat in very stark terms.

I believe that this change has come about because these senior officials have determined that the situation has become so dangerous, as our networks and technology and companies become so interconnected, that they understand that public awareness is increasingly critical to dealing with this threat.

For example, last month during an appearance before the Senate Select Committee on Intelligence FBI Director Robert Mueller said that while terrorism is the greatest threat today, "down the road, the cyber threat will be the number one threat to the country."

A 2010 Pentagon report found "… [i]n the case of key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia, the Peoples Republic of China resorts to more focused efforts, including the use of its intelligence services and other-than legal means, in violation of U.S. laws and export controls."

The report also highlighted China's cyber-espionage efforts. The U.S. intelligence community notes that China's attempts to penetrate U.S. agencies are the most aggressive of all foreign intelligence organizations.

Other senior U.S. military and intelligence officials have become increasingly vocal about their concerns about the scope of Chinese espionage and cyberattacks. Defense Intelligence Agency chief General Ron Burgess also recently testified that "China has used its intelligence services to gather information via a significant network of agents and contacts using a variety of methods... In recent years, multiple cases of economic espionage and theft of dual-use and military technology have uncovered pervasive Chinese collection efforts."

Last year, the usually-reticent Office of the National Counterintelligence Executive issued a warning that "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The counterintelligence office took this rare step of singling out the Chinese due to the severity of the threat to U.S. national and economic security.

And a March 8, 2012 Washington Post article described how "[f]or a decade or more, Chinese military officials have talked about conducting warfare in cyberspace, but in recent years they have progressed to testing attack capabilities during exercises… The (PLA) probably would target transportation and logistics networks before an actual conflict to try to delay or disrupt the United States' ability to fight, according to the report prepared by Northrop Grumman" for this commission -- and I want to commend this commission for requesting and publishing this important research.

We are beginning to witness the consequences of the cyber threat. According to a March 13, 2012 New York Times article "[d]uring the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago."

In an interview with The New York Times, Homeland Security Secretary Janet Napolitano said "I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming. The information on a cyberattack is at the same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

Notably, Chinese espionage isn't limited to government agencies. In an October 4, 2011 Washington Post article, Chairman Mike Rogers remarked: "When you talk to these companies behind closed doors, they describe attacks that originate in China, and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity."

Cyberespionage is having a real and corrosive effect on job creation. Last year, the Washington Post reported that, "[t]he head of the military's U.S. Cyber Command, Gen. Keith Alexander, said that one U.S. company recently lost $1 billion worth of intellectual property over the course of a couple of days – 'technology that they'd worked on for 20-plus years – stolen by one of the adversaries.'"

The record is clear: what policymakers used to reticently refer to as the "Advanced Persistent Threat" is now increasingly acknowledged as China's asymmetric warfare and economic strategy against the U.S.

Because of our past reluctance to acknowledge the severity of this issue, the Congress and the administration are now struggling to keep up. As many are aware, several comprehensive cybersecurity bills are stalled in the Senate amid jurisdictional and partisan wrangling.

The House is quietly trying to advance more targeted bills and I want to commend my colleagues Mike Rogers, chairman of the Intelligence Committee, and Peter King, chairman of the Homeland Security Committee, for their excellent leadership on this issue.

As chairman of the House Appropriations subcommittee that funds the FBI, Commerce Department and the National Institute for Standards and Technology (NIST), my subcommittee has also been funding some of the key civilian and law enforcement agencies involved in the fight against the cyber threat.

That is why I prioritized cybersecurity programs in the fiscal year 2012 Commerce-Justice-Science Appropriations bill, including significant increases to the FBI's joint cyber task force and requiring each agency to vet its IT equipment purchases. I also directed the FBI to produce an annual unclassified cyber report.

I am planning take even more significant steps in the fiscal year 2013 bill that is currently under development, including adopting many of this commission's recommendations.

Although the government and the private sector have finally come to appreciate this threat and start to take the necessary steps to address it, the threat is evolving and I am concerned that we may continue to be behind the curve.

One issue that the U.S. has failed to develop a coherent and strategic policy to address is the unique and unprecedented threat from Chinese state-owned or state-directed companies that are operating in the U.S. I believe this threat is particularly pronounced from Chinese telecom firms.

Earlier this year, The Economist magazine published a special report on Communist Party management of Chinese corporations. The article noted the Chinese government's particular support for its telecom and IT industry noting that, "the end result is the creation of a new class of state companies: national champions that may not be owned by governments but are nevertheless closely linked to them"

The article reported that "[t]he (Communist) party has cells in most big companies – in the private as well as state-owned sector – complete with their own offices and files on employees. It holds meetings that shadow formal board meetings and often trump their decisions"

According to The Economist, the Chinese government even has an expression for this strategy: "The state advances while the private sector retreats."

Author Richard McGregor wrote that the executives at major Chinese companies have a "red machine" with an encrypted line to Beijing next to their Bloomberg terminals and personal items on their desks.

Given this level of party control in China's private sector, we shouldn't be surprised to learn that the PLA has been operating cybermilitias out of telecom companies.

Last year, The Financial Times reported that the PLA has even documented how it will use telecom firms for foreign espionage and cyberattacks.

A paper published in the Chinese Academy of Military Sciences' journal noted: "[These cyber militia] should preferably be set up in the telecom sector, in the electronics and internet industries and in institutions of scientific research," and its tasks should include "stealing, changing and erasing data" on enemy networks and their intrusion with the goal of "deception, jamming, disruption, throttling and paralysis."

The same article also documented the growing number PLA-led cyber militias housed in "private" Chinese telecom firms.

The article reported on one example at the firm Nanhao [Nan-how]: "many of its 500 employees in Hengshui [Hang-shoo], just south-west of Beijing, have a second job. Since 2005 Nanhao has been home to a cybermilitia unit organized by the People's Liberation Army. The Nanhao operation is one of thousands set up by the Chinese military over the past decade in technology companies and universities around the country. These units form the backbone of the country's internet warfare forces, increasingly

seen as a serious threat at a time of escalating global cybertensions."

That is what makes me so concerned about Chinese telecom firms' growing operations in the U.S. market. Chinese state-directed are collaborating and cooperating with the Chinese government to a degree that would be unfathomable in the U.S. or other Western economies.

And as those Chinese state-backed firms enter the U.S. market, it is unclear whether they will be playing by our rules, or their own.

Currently, the most concerning of these Chinese telecoms is Huawei, which is attempting to increase its market share in the United States and around the world. Numerous government reports have linked Huawei's corporate leadership to the Chinese intelligence services and the People's Liberation Army (PLA), raising concerns about Huawei networks and devices being subject to espionage by the Chinese government.

These connections are particularly noteworthy given Huawei's rapid rise as a telecom giant. According to a March 18 article in the Wall Street Journal, "Huawei Technologies Co. has almost doubled its work force over the past five years as it strives to become a mobile technology heavyweight."

The article also noted that "Huawei's network business has thrived at the expense of struggling Western network companies such as Alcatel-Lucent Co. and Nokia Siemens Networks. Initially, Huawei supplied low-cost phones to telecommunications operators in the West under their own brand, but over the past year, Huawei has also been quietly building and investing in its own brand of high-end smartphones and tablets."

Huawei executives make no secret of their goal to dominate the telecom market. In a March 6, 2012, interview with the technology news Web site, Engadget, Huawei device chief Richard Yu said "[i]n three years we want Huawei to be the industry's top brand."

However, Huawei's growth in the U.S. market should give all Americans serious pause. Last week, respected national security reporter Bill Gertz wrote in The Washington Free Beacon about this commission's recently released cybersecurity report.

Gertz wrote: "[n]ew information about Chinese civilian telecommunications companies' close support of the Chinese military and information warfare programs is raising fresh concerns about the companies' access to U.S. markets, according to a report by the congressional US-China Economic and Security Review Commission."

"One of the companies identified in the report as linked to the PLA is Huawei Technologies, a global network hardware manufacturer that has twice been blocked by the U.S. government since 2008 from trying to buy into U.S. telecommunications firms," Gertz continued. "Huawei is a well established supplier of specialized telecommunications equipment, training and related technology to the PLA that has, along with others such as Zhongxing, and Datang, received direct funding for R&D on C4ISR [high-tech intelligence collection] systems capabilities."

The report further added, "[a]ll of these [Chinese telecom] firms originated as state research institutes and continue to receive preferential funding and support from the PLA."

Huawei's efforts to sell telecom equipment to U.S. networks have long troubled the U.S. defense and intelligence community, which has been concerned that Huawei's equipment could be easily compromised and used in Chinese cyberattacks against the U.S. or to intercept phone calls and e-mails from American telecom networks.

According to a 2005 report by the RAND Corporation, "both the [Chinese] government and the military tout Huawei as a national champion," and "one does not need to dig too deeply to discover that [many Chinese information technology and telecommunications firms] are the public face for, sprang from, or are significantly engaged in joint research with state research institutes under the Ministry of Information Industry, defense-industrial corporations, or the military."

In fact, in 2009, The Washington Post reported that the National Security Agency "called AT&T because of fears that China's intelligence agencies could insert digital trapdoors into Huawei's technology that would serve as secret listening posts in the U.S. communications network.

Over the last several years, Huawei's top executives' deep connections to the PLA and Chinese intelligence have been well documented. As Gertz summarized in his article, "a U.S. intelligence report produced last fall stated that Huawei Technologies was linked to the Ministry of State Security, specifically through Huawei's chairwoman, Sun Yafang, who worked for the Ministry of State Security (MSS) Communications Department before joining the company."

That is why senior administration officials in the Bush and Obama administrations have repeatedly intervened to block Huawei's access to U.S. networks. "In 2008, the Treasury Department-led Committee on Foreign Investment in the United States (CFIUS) blocked Huawei from purchasing the U.S. telecommunications firm 3Com due to the company's links to the Chinese military," Gertz reported.

"Last year, under pressure from the U.S. government, Huawei abandoned their efforts to purchase the U.S. server technology company 3Leaf. In 2010, Congress opposed Huawei's proposal to supply mobile telecommunications gear to Sprint over concerns that Sprint was a major supplier to the U.S. military and intelligence agencies."

When the White House, Intelligence Community, Defense Department and the Commerce Department all have worked to block Huawei from gaining greater access to U.S. networks, the American people should take notice.

In all my years in Washington, very rarely have I seen the defense, intelligence and civilian agencies come together in such a quiet but concerted effort to warn of a security threat from a foreign entity.

It's not just Huawei's longstanding and tight connections to Chinese intelligence that should trouble us.

Huawei has also been a leading supplier of critical telecom services to some of the worst regimes around the world. Last year, the Wall Street Journal reported that Huawei "now dominates Iran's government-controlled mobile-phone industry…it plays a role in enabling Iran's state security network."

Gertz reported that Huawei has also been "linked to sanctions-busting in Saddam Hussein's Iraq during the 1990s, when the company helped network Iraqi air defenses at a time when U.S. and allied jets were flying patrols to enforce a no-fly zone. The company also worked with the Taliban during its short reign in Afghanistan to install a phone system in Kabul."

Given all of this information, there should be no doubt Huawei poses a serious national and economic security threat to the U.S. It is no secret that the Peoples Republic of China has developed the most aggressive espionage operation in modern history, especially given its focus on cyberattacks and cyberespionage.

Perhaps that is why Beijing has ensured that Huawei is able to continue its global market growth by "unsustainably low prices and [Chinese] government export assistance," according to this commission's January 2011 report on the national security implications of Chinese telecom companies.

Due to China's secrecy, the full extent of Huawei's subsidies are not fully known. But given its unrealistically low prices, it remains unknown whether Huawei is even making a profit as it seeks to dominate the telecom market. Why would the Chinese government be willing to generously subsidize such unprofitable products?

The American people have a right to know whether their government is doing everything it can to protect their cell phone and data networks.

But I fear that with Huawei's rapid growth in the U.S. market, we may soon find that we are too intertwined with Huawei network equipment and devices to address potential security concerns. We must resolve these concerns before Chinese telecom firms make significant inroads on U.S. networks, not after.

And as Huawei increases its lobbying presence in Washington, members should be fully aware of the firm's intimate links to the PLA and the serious concerns of our defense and intelligence community.

Verizon, Sprint, AT&T, T-Mobile and other U.S. network carriers should not be selling Huawei devices given these security concerns. But if they do, they have an obligation to inform their customers of these threats. This is especially important when carriers are selling Huawei phones and tablets to corporate customers. They have a right to know that Beijing may be listening.

Thank you again for the opportunity to testify this morning. I look forward to working with this commission as we continue to address this challenge.

HEARING CO-CHAIR WORTZEL: Mr. Healey. Thank you.

OPENING STATEMENT OF JASON HEALEY
DIRECTOR, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL

MR. HEALEY: Thank you very much. Good morning, Commissioners. Happy Monday morning. Thanks for the opportunity to be here.

The government is finally, finally becoming more clear-minded about the risk of Chinese espionage and is rushing towards a solution, and I don't doubt the hard work, the patriotism of those people in the executive branch as they're plowing ahead on this, but it's not clear that we're heading in the right direction.

The threat of Chinese espionage is so critical that General Alexander has called it "the biggest transfer of wealth through theft and privacy in the history of mankind"--the history of mankind. So bad, in fact, that the government might have to start regulating the private sector, and our companies might have to submit their communications to government monitoring.

But the threat is not so bad apparently to interest the government in the history of how we got here, or to go enough on the record about the threat to take risks to share needed information, or be willing to tell the Chinese to back off, and I call these the government's four silences. Added together, I fear they're driving us to defeat.

First, silence about how we got here. This silence is more of ignorance than interaction. When I meet with them, too many of America's cyber-warriors and policymakers feel the problem started somewhere around 2003 to 2008. That is roughly when they personally got involved.

It turns out that we're so busy rushing into the future we haven't bothered to really look back and figure out the lessons from the past, so no wonder we keep having to learn new wake-up calls.

So our understanding of the basic issues is as old as I am: the Defense Science Board that first discussed hardware or software leakages, intrusions, supply chain attacks and appropriate risk levels was researched in 1969 and published in 1970. Forty years, and we're still struggling to understand this.

We know we face patient and motivated adversaries with extensive researchers that are adept in circumventing safeguards. Those exact phrases come not from any recent NCIX report about the Advanced Persistent Threat, but the National Research Council from 1991, the year that I got commissioned in the Air Force.

So for more than 20 years, the executive branch has understood APT threat, and yet we're still struggling and treating it like it's new.

America suffered its first state-sponsored espionage case not in 2003 but in the mid-1980s. Our first Title 10 combat unit conducting offense and

defense stood up in 1995, not 2005, and we had a joint warfighting cyber commander in 1998, not 2008.

Looking back should teach us important lessons, perhaps the most important of which is we're stuck in a cycle of suffering. If we're going to learn from this history, we need to collect it and teach it. I've started a history series with the Atlantic Council starting with "Lessons From Our First Cyber Commanders" and am the principal investigator for the first cyber conflict history book.

The government needs to begin its own effort to go out, to collect this history, start the oral histories with some of these commanders and other founding members that we can learn from it.

And just like military officers have to learn their history--Rich and I were at the Air Force Academy--we had to learn the lessons of the early air pioneers and be able to apply them today, learn the early air campaigns and units, and be able to apply those lessons to today--we have to do the same thing for today's cyber warriors. The military needs to do this. DHS needs a companion program to help make sure their people understand.

Second, silence about the threats we face. Government officials seem keen to leak info on how bad Chinese espionage is, but unwilling to actually tell the American people or our companies and critical infrastructure. If espionage is such a problem, how come we have to hear about it from the press or from experts like those sharing this panel with me today? Thank goodness for the Commission's reports.

When I ask the executive branch why they can't say more, I get a range of overlapping but insufficient reasons:

We are sharing; didn't you see the NCIX report? I have no opinion; it's classified above my level. We'd like to share; it's caught up in interagency. We can't prove it's China. If we say China is doing it, they may get angry and stop lending us money. There's nothing illegal about spying. If we declassify what we know of the threat, people would panic. The private sector isn't sharing with us, so why should we share with them? My response of "government for the people" wins that argument less than you might imagine.

If we discussed this, it wouldn't matter since the Chinese won't change their behavior. It's a wilderness of mirrors. If we discussed this, then the Chinese would know that we know that we know that they know. If we talk, then our intelligence take wouldn't be quite as good.

None of these reasons singly or in combination can possibly be sufficient given how badly we're losing. If the private sector is truly critical, we have to change our mind-set. We treat this as a state secret even from those under attack. The government is creating our own "wilderness of mirrors" built entirely around itself. We're not facing a single monolithic KGB, but a splash of

non-state hacker groups loosely affiliated with different official organs of the Chinese state.

Government must follow the example of this Commission and be clear about the depth of the problem and name the problem involved: China. We'll never make progress if everyone looks for their classification stamps when the words "China," "cyber," and "espionage" are used together. The spy-versus-spy mentality is driving us into defeat. We have to take every opportunity to be clear and public about what we face.

Third, silence about practical information which could help the private sector. While the government has started projects, most notably the DIB cyber pilot to share NSA's signatures of malicious software, these require security clearances and secure facilities. They likely increase our work factor more than that of our adversaries.

We have to shift the government's mind-set to seeing the private sector as the "supported command" rather than the "supporting command." Too many of the government's plans put the government at the center and look to the private sector to give the government support, and that's obviously the reverse of what's needed.

As one bold step, we could simply declassify the signatures. After all, the bad guys have themselves already made their malicious software public by releasing it, so sources and methods should not be a significant problem, be less expensive in the long run, and would bolster rather than supplant the security market.

Last, silence to the Chinese about our increasing fury. I was at a recent event at Georgetown that had both China cyber and nonproliferation people, or people that have dealt with China on these issues. The nonproliferators were able to draw on a range of conversations they had with the Chinese. When we talked to them about Iran or North Korea, they're helpful. When we talk about Pakistan, they're not helpful. Sometimes it helps if we go really public and splashy. Other times it helps if we go really quiet, and we make sure it's not in the press.

When we talked to the cyber people, we found out there has been nothing similar, nothing like that kind of conversation with the Chinese. We've mentioned it to them, as I've been told Vice President Biden did, but not a range of conversations like the nonproliferation people found to be very successful.

If this is as bad as we say it is, if this is so bad we might have to pass new laws to regulate the private sector, and we're keeping it private, I mean secret from the private sector, we have to bring it up in every opportunity that we can, to poke the Chinese in the chest publicly and private to say regardless of whether this is actually your government doing this, you must help us stop it because frankly it's getting towards one of our red lines.

Thank you.

PREPARED STATEMENT OF JASON HEALEY
DIRECTOR, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL

The Government's Four Cyber Silences

Testimony of

Jason Healey

Director, Cyber Statecraft Initiative, Atlantic Council to the

US-China Economic and Security Review Commission on

"Developments in China's Cyber and Nuclear Capabilities"

Monday, March 26, 2012
George Mason University, Manassas, Virginia

Thank you for the opportunity to be here.

I am going to speak very plainly today. The government is finally becoming more clear-minded about the risks of Chinese cyber espionage and is rushing towards solutions. And while there is no doubting the hard work and patriotism of those behind these efforts, it is not clear we are heading in the right direction.

The threat of Chinese espionage is so critical that the commander of our military cyber defenses has called it the "the biggest transfer of wealth through theft and piracy in the history of mankind." It is so bad, in fact, the United States may need to regulate the private sector and our companies need to submit to government monitoring.

But the threat has *not* bad enough to interest the government in the history of how we got here, or enough to go on the record about the threat, to take risks to share needed information or be willing to tell the Chinese to back off.

I call these the government's Four Silences. Added together I fear they are driving us to defeat.

First: **Silence about how we got here**. This silence is more of ignorance than inaction. When I meet with them, too many of America's cyber warriors and policy makers feel the battle only started sometime between 2003 and 2008 – that is, roughly when they personally got involved. We have been breathlessly rushing into the future, rarely looking back to learn what has happened before. No wonder we keep having new wake-up calls.

Our understanding of the basic issues is as old as I am. The Defense Science Board report that discussed hardware and software leakages, intrusions, supply chain attacks, and risk levels was researched *in 1969*. And yet we're still struggling.

We know we face adversaries that have "extensive resources in money, personnel, and technology;" and are "adept in circumventing physical and procedural safeguards," "patient and motivated," and "capable of exploiting a successful attack for maximum long-term gain." However, those exact phrases come, not from any recent NCIX report, but the 1991 "Computers at Risk" report from the National Research Council.

For more than 20 years, then the Executive branch has understood the advanced persistent threat … and yet we're still struggling.

America had its first state-sponsored cyber espionage case not in 2003, but in the mid-1980s. Our first Title 10 combat unit conducting offense and defense stood up in 1995, not 2005. We had a joint warfighting cyber commander in 1998 not 2008.

We treat cyber as forever novel and so we can't learn any lessons. No wonder we're forever struggling. Looking back should teach us important lessons, perhaps the most important of which is we're stuck in a cycle of suffering.

If we're going to learn from this history we need to collect it and teach it. The Atlantic Council has

started a history series, starting with "Lessons from the First Cyber Commanders" to help and I am principal investigator with the Cyber Conflict Studies Association on the first cyber conflict history book. The US government should begin their own efforts, to collect key documents, conduct oral histories with the first generations of cyber warriors and start codifying the lessons learned.

And just as today's military officers learn the lessons of Cannae, Trafalgar, the Chosin Reservoir, and MIG Alley, so must DoD's new cyber cadre study *yesterday's* cyber operations to understand those of *tomorrow*. This history should be part of the professional military training of our new military officers and a core part of the curriculum in courses to build military cyber warriors. DHS should likewise include this in their own coursework as part of their education projects to ensure it reaches the civilian workforce.

Second: **Silence about the threat we face**.

Government officials seem keen to *leak* information on how bad Chinese espionage is, but unwilling to actually *tell* the American people or our companies in critical infrastructure. If espionage is such a problem, how come we have to hear about it from the press or from experts like those sharing this panel with me today? Thank goodness for the Commission's reports.

When I poke government officials about this, they get giddy about trifles, a few sentences in an NCIX report or pat themselves on the back because a few members of industry in critical sectors have received security clearances and get periodic briefings. These are worthy achievements, but pale before the problem.

When I ask *why* the Executive branch cannot say more, I get a range of overlapping but contradictory responses:

1. We *are* sharing, didn't you see those sentences in the NCIX report?
2. I have no opinion and can't discuss this: it is classified way above my pay grade.
3. We would like to but it is caught up in the interagency.
4. We can't prove it's really China.
5. If we say China is doing it, they may get angry and stop lending us money.
6. There's nothing illegal about spying; after all, we do it!
7. If we declassified what we knew of the threat, people would panic.
8. The private sector isn't sharing with us, so why should we share with them? (Somehow, my response of, "government for the people" wins that argument less than you'd imagine.)
9. If we discussed this, it wouldn't matter since the Chinese would not change their behavior.
10. It's a wilderness of mirrors. If we discussed this, then the Chinese would know that we know.
11. If we talk, then our intelligence take won't be as good.

None of these reasons given, singly or in combination, are sufficient given how badly we're losing. If the private sector is truly critical, we have to change our mindset to be able to discuss the problem. Intelligence officers love to collect, more and more, and if they act it on that collection it might disrupt the flow. But by treating this problem as a state secret, even from those under attack, the government is creating our own wilderness of mirrors, built entirely around itself. Worse, this familiar counterintelligence game is one our adversaries do not even know. We are not facing a single, monolithic KGB but a splash of non-state hacker groups loosely affiliated with many different official organs of the Chinese state.

What must be done? The government must follow the example of the Commission and be clear about the depth of the problem and name the country involved: China. If it is time for action we need to take this out of intelligence and counterintelligence channels and declassify significant portions, something

that can only be done from the top.

We will never make progress if everyone looks for their classification stamps when the words "China," "cyber" and "espionage" are used together. ***The spy-versus-spy mentality is driving us into defeat.*** Given that it has said so little, no wonder there are so many skeptics of the government's motives. If the administration wants America to take it seriously, it must be clear: repeated speeches from senior officials, not just occasional sound bites; not just one NCIX report, but a slew of them; not just leaks to media, but interviews. The frequency and seriousness of their statements need to match the crisis at hand and this should start from the White House.

Third: **Silence about practical information which could help the private sector**.

A related point to the one I just made is that the government has been far too cautious giving needed practical information to the private sector. The reasons are usually the same, but the impact affects their day-to-day defenses. When the private sector does not share, then they are either not patriots or too fixated on their shareholders. When the government does not share, it is okay, because it is classified, stuck in the interagency, someone else's job, or we had a Deputies Committee say it was permissible to not share it for intel gain/loss.

In cyber conflict, the offense already begins with a head start. To beat them, the defenders need to significantly increase the bad guys' work factor more than their own. While the government has started projects, most notably the DIB cyber pilot to share NSA's signatures of malicious software, these typically don't easily scale, requiring security clearances and secure facilities. They likely increase our work factor probably more than our adversaries.

Indeed, a recent study found that only 1% of NSA's signatures shared with the Defense Industrial Base

were novel. How many hours were spent in interagency meetings for that one percent? Some in Congress and the military seem to want constitutionally troubling government monitoring of private sector companies, but does this make sense for marginal gains?

The fix is to shift the government's mindset: in cyber conflict, the private sector is usually the "supported command" not the "supporting command." They are the targets, the ones fighting in the trenches every day, and if we want to win they need more help. Think about past cyber crises: in how many did the solution depend primarily on government solutions? In most cases, the critical solutions instead came from McAfee, or Microsoft, not from any a department or agency. The exceptions tend to be attacks that predominantly only affected the government to begin with. Yet too many of the government's plans put the government at the center, and look to the private sector to give support. This is the reverse of what is needed: it is the private sector that will fix the problem and the government should be supporting them.

To put it another way, we are finishing two major wars. When American soldiers have been in harm's way, intelligence agencies will take significant risks to declassify the right information to keep them safe. Though it is a different kind of fight, the US government should be willing to take similarly bold risks to support our embattled companies on the front lines against Chinese espionage.

As just one example of how to do this, we should simply declassify the signatures. After all, by releasing their attacks "in the wild" over the Internet, *the bad guys have themselves already made their malicious software public*. This will be far less expensive in the long run and more effective as it would bolster, not supplant, the security monitoring market.

This leads us to the last silence.

Fourth: **Silence to the Chinese about our increasing fury**.

A recent event at Georgetown University discussed the US experience dealing with China both for WMD non-proliferation and for cyber. The non-proliferation experts explained their long dialog with the Chinese on this sensitive topic, through which they learned some keys to success.

By drawing on a range of discussions, some successful and some not, these negotiators discovered the Chinese government was more willing to limit proliferation to some countries but not others. Sometimes they discovered a discrete word to the Chinese leadership would work, while other times public shaming was needed. They still haven't figured everything out, of course, but they can point to progress in influencing Chinese behavior.

When asked the same question, America's cyber experts answered with a sheepish look, admitting that we have not yet told the Chinese leadership, in any similar fashion, that we are upset with their activities against us. We have mentioned it to them, but rarely more.

How can this be? The first answer I receive is usually that we don't want to upset the Chinese. After all, they own bazillions of US Treasury bonds. But is it true the United States is willing to square off against China on tire imports and rare earths, but not on "the biggest transfer of wealth through theft and piracy in the history of mankind" in General Alexander's words?

We don't need to pick an international fight (or perhaps we do) but at least, let's start the official dialog. We must raise Chinese cyber espionage in every military-to-military dialogue, in ever JCCT meeting, in the Strategic and Economic Dialogue, and with visits from all of their state leaders. How can we say we are trying to stop their espionage by doing anything less? How can we even *consider* government monitoring of private networks before our own government has even told the Chinese they need to back off? Better yet, we can choose from at least the United Kingdom, Australia, Germany, France and Canada to be a good cop to counter our bad cop routine.

Better yet, we don't have to prove without doubt that every single espionage case is coming from China or that the Chinese government itself is conducting them. The Atlantic Council just published a ten-point spectrum to help assign responsibility for cyber events (see table 1). This is just one tool that can help us address the forest of Chinese intrusions, rather than the trees of the forensics of each case. As a national security matter, we can simply decide to not care if these are sponsored by the Chinese government or not. If the government (and private sector) releases sufficient evidence showing the incidents are sourced from that country, the administration can just hold them responsible to make it stop. This approach of "national responsibility" is likely to be far more effective than forcing ourselves to jump over the needlessly high bar of proving technical attribution.

Table 1:
The Spectrum of State Responsibility

1. **State-prohibited**. The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate**. The national government is cooperative but unable to stop the third-party attack
3. **State-ignored**. The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped**. Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated**. The national government coordinates third-party attackers such as by "suggesting" operational details
7. **State-ordered**. The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted**. Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed**. The national government conducts the attack using cyber forces under their direct control
10. **State-integrated**. The national government attacks using integrated third-party proxies and government cyber forces

Conclusion

The Administration and Congress are taking cyber espionage seriously, more seriously than they have in years. Yet it is far from clear we are doing enough or heading in the right direction.

We must at least tackle these four cyber silences:

1. Silence about how we got here
2. Silence about the threat we face
3. Silence about practical information which could help the private sector
4. Silence to the Chinese about our increasing fury

These will not by themselves solve the problem, but at least we will all understand the scope of the problem and have us towards solutions that may break the cycle of suffering. To win, we must speak. To speak we have to declassify. To declassify we must be bold. And we must do this today.

PANEL I – QUESTIONS AND ANSWERS

HEARING CO-CHAIR WORTZEL: Well, thank you very much, all three of you, especially for putting in practical recommendations.

I want to ask Mr. Healey, if I might, when I look at some of your other writings, you seem to advise that the U.S. should hold governments responsible and not focus so much on attribution even if we can't attribute to a specific organization.

And if I've characterized it right, I wonder if you could explain that view and whether there are legal steps such as General Cartwright outlined that we should be taking?

And if the others have thoughts on this, please contribute.

MR. HEALEY: Thank you very much, Commissioner.

This was one of my recent publications, and I brought extra copies for Commissioners or for attendees, that says I don't think diplomats or generals should ever use the word "attribution."

Attribution is important if you're a security researcher. It's important if you're law enforcement because it helps you find out the person responsible. The word "attribution" makes us start thinking we have to begin at the technical level and then work our way up, and maybe at the end of that process, we can find out if there was a government responsible.

I think for diplomats and generals, that's a sucker's game, and we shouldn't play it. Look at Estonia. Forensically, we were told that 178 countries had servers that were responsible in the attack. That is not helpful. That is forensic information that clouds the fact that if the president wanted to make that attack stop, he had to do one thing, or he had to start in one place, and that was pick up the phone and call the Kremlin. 178 countries didn't matter. One country mattered. Russia.

So that's what I say, we don't have to play the game of difficult attribution. It's an important step, and we need to continue also doing that, but if I were in the situation room, again, advising the president when this happens, or let's take it to Chinese espionage--I'm sorry--let's be direct about this--we don't have to prove that the Chinese government is behind any of this. We have enough evidence from security researchers and from our own intelligence to come out and say, look, enough is enough. We don't care if you're behind it or not, but there is enough that shows that Chinese citizens and organizations are involved. We are getting to a red line. Please make it stop.

HEARING CO-CHAIR WORTZEL: Thank you.

Anything to add on that?

MR. BEJTLICH: I would add that for cases where you can say this is a serious problem, that it does make sense to contact the country that you believe

is responsible. I think that there's a range of that that happens in the non-cyber world. I mean clearly what happened after 9/11 is we felt that Afghanistan was harboring a group of people that we did not like, and it reached the level of "we're going to do something about that."

I think that there are probably cyber equivalents where you can say this is such a problem, and maybe it doesn't have to be a major cyber attack, it could simply be a pattern of activity over many years, which is what we've had now for the last seven, eight, nine years, that you could say we have identified the following systems. Consistently over the course of that time, they have been involved in the death-by-a-thousand-cuts sort of economic espionage, and we would want you to take them down.

I was actually shocked this morning to hear General Cartwright mention that we had done something like that in China. My company, we could probably provide lists of infrastructure we would like taken down if--

HEARING CO-CHAIR FIEDLER: That's why I asked the question.

[Laughter.]

MR. BEJTLICH: --it's such a possibility.

MR. VILLENEUVE: Yes. From a purely technical perspective, I've actually personally had decent luck dealing with the Chinese server to get individual servers turned off. I treat it like a normal botnet case, as I would in any other, and report it as malicious activity, and they usually shut them down.

The problem is that we used to see a lot of servers actually hosted in China, but now we see them hosted all over the world, a lot actually in the United States.

Now, of course, determining who's controlling these servers is a different question. But even that, there's been some fantastic work by Joe Stewart looking at the originating IP addresses of those who are controlling sort of intermediary servers that were hosted in third countries. So there is more work to be done there. I think the trick is whether a lot of the law enforcement agencies who would be responsible for shutting these down would rather keep them up and watch them or shut them down for defensive purposes.

HEARING CO-CHAIR WORTZEL: Thank you very much.

Commissioner Shea, or Chairman Shea.

CHAIRMAN SHEA: Thank you. Thank you for your testimony, all three of you.

I just want to get at the point that you're making, Mr. Healey. You mentioned General Alexander's quote saying that this is the biggest transfer of wealth through theft and piracy in the history of mankind. We're familiar with the NCIX report of last October.

Reading an op-ed from the former Director of the NSA, the head of Homeland Security, and Deputy Secretary of Defense:

The Chinese government has a national policy of economic espionage in cyberspace. In fact, the Chinese are the world's most active and persistent practitioners of cyber espionage today. And then they say this costs us easily billions of dollars and millions of jobs--these three individuals who are responsible for our nation's national security.

And then I hear from General Cartwright that we should, the government should, prospectively engage in a dialogue on this issue, and if this is that big a deal, why haven't we raised this issue with the Chinese directly? I'm beginning to think maybe it's not that big a deal, and this is just a lot of hyperbole.

If all these statements are true, I'm just sort of mystified as to why this is not at the center of our relationship and discussions. All three of you if you can answer.

MR. HEALEY: It mystifies me also that we're willing to poke about so many different WTO cases, whether it's solar panels or tires, and I know tires can be important, but many other issues, we're willing to poke the Chinese about, but not for this.

I think it's because the spy/counter spy, the counterintelligence mentality, that if we share this, then we might lose some collection, and that really disappoints me having spent so much time in the private sector, having been a taxpayer and a taxpaying company, to find out that we're being allowed to suffer in the private sector so that our intelligence community can get better take, so that our spying can be a bit better.

The benefits of espionage predominantly accrue to the government. The espionage that we're seeing penalizes primarily the private sector, and I think that's an imbalance that we can no longer afford.

MR. BEJTLICH: I would agree with that. We just don't have a construct for thinking about this. Right now, my company is responding to somewhere between 12 and 16 intrusions that are serious. We don't take small work. We take the worst of the worst, and we work to keep that out of the news. So these are companies that they do not want to be known that their most sensitive intellectual property is now overseas, and these are all companies that have had this happen. These are all intrusions that started last year or earlier, so we just don't know how to think about this.

And these companies don't know how to think about it. We have conversations where they say “we just lost all this data.” It takes them months to try to figure out what the economic value is, and then they make decisions or they think about decisions like “do we have to sell ourselves to a larger company in order to preserve some type of shareholder value in the event that this gets out in six months or a year?”

I mean these are the sorts of conversations we're having that no one

knows how to think about it, and very rarely does it get to the level of a CEO making a decision, well, "I'm just not going to do business in China anymore." Most of these companies still continue to do business.

MR. VILLENEUVE: I'll just quickly echo what's been said. In the security community, we're often under NDAs or we have customers who have privacy to protect, and a lot of us report, we disclose compromises directly to the victims, and that's a tough job to phone somebody up and tell them that they've been breached, and a lot of this is happening, but there is no sort of public record of it, which is why people think that we're often overstating the problem.

MR. HEALEY: If I may, if a private company doesn't share, then it's too beholden to its shareholders or it's beholden to China or they're not patriots. If the government doesn't share, it's intel gain loss and the deputies committee said it was okay.

HEARING CO-CHAIR WORTZEL: Mr. Wolf has arrived. He's going to start at 11, so we're going to continue with questioning, and then a couple minutes before that I'll break, and we'll get ready for him.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you, gentlemen, for being here. I hope that you--I have probably a number of hours of questions--that you'll be willing to respond to a much shorter subset in writing later for anything that we may not get to with the panel today.

I wanted to ask a question of the whole panel starting with you about the movement towards the cloud, which, in the desire to reduce the federal budget deficit, there is a view that going to the cloud has enormous cost savings, and it certainly does, but the lateral movement of data within a cloud is actually pretty significant--correct me if I'm wrong--from a technical perspective. You don't have a dedicated server in the cloud. Data is written to the next available whatever, and the software makes sure that your data is, in fact, relayed back to you upon demand.

So the ability, as I understand it, for cyber intrusions or cross-migration and the ability to get somebody else's data is probably pretty significant if you go into rootkits or anything else within a server farm within the cloud, so to say.

Last week I saw an article from the Australian press, Chinese technology giant Huawei has been banned by the federal government from participating in tenders worth billions of dollars to supply equipment to the national broadband network, et cetera, stemming from concerns that doing business with Huawei could make the NBN vulnerable to cyber attacks originating in China.

I asked that question of the General before. What should we be looking at in terms of the supply chains, and now moving towards the cloud, that

the provision of the equipment, are those new vectors for attack? Should we be looking at them any differently than we look at the current phishing malware, other attacks? Is that an increasing problem, decreasing? How should we be looking at it? And each of the panelists if you could?

MR. BEJTLICH: Sure. The cloud is one of the most complicated--I mean if enterprise security wasn't already complicated, factoring in the cloud makes it exceptionally more complicated.

There's a complex set of tradeoffs here. If you're a small company or mid-size company, and you have zero to one security people or perhaps zero to one IT people, you get a definite advantage in security going to the cloud because you would imagine the cloud people have something security- wise.

COMMISSIONER WESSEL: Firewalls or anything else that you may not want to spend the money on.

MR. BEJTLICH: Absolutely.

COMMISSIONER WESSEL: Yes.

MR. BEJTLICH: So for many of the companies that we're seeing hit now, there's a big advantage to going to the cloud because you're just better off.

However, at the higher end when you can staff a team, what happens is when you go to the cloud, you tend to lose visibility. You can't inspect your own equipment now to see what the state of it is because it's all hosted someplace else.

And again, you have to sort of differentiate between what's cloud, what's hosted. We have seen the Chinese actors going after hosted environments. In other words, equipment that is controlled by an organization, but it's housed someplace else. So we have seen that happening.

We haven't seen attacks against sort of pure cloud like a SalesForce.com or something like that. But as the data is increasingly in those places, I'm sure we're going to see it. Well, I say we'll see it, but that's really the problem as well. Who will see it? The victim probably won't.

I mean, can you tell when you use your Gmail account if someone has been there looking at your e-mail? Probably not. I mean, guess what, Gmail hardly knows either. So those are the challenges I see.

COMMISSIONER WESSEL: But then the intersection between, again, an increasing movement to the cloud and the globalization of supply chains--

MR. BEJTLICH: Right.

COMMISSIONER WESSEL: --again, as you're pointing out, it moves out of your shop to somewhere else. Small guy, yes, it's better for the government.

MR. BEJTLICH: Yeah.

COMMISSIONER WESSEL: Does that increase the security risks or decrease them? What's your view about the intersection there?

MR. BEJTLICH: I would say overall there is, I'll just tell you what we're

doing. We're moving our e-mail in-house. I feel that if you can run it yourself, you're going to gain the security benefit. We saw with the Aurora attacks, they went after Gmail to get the dissident e-mails. So we're going to see more of that as more people put sensitive data in those locations.

MR. VILLENEUVE: I can't really expand too much on what Richard just said, but what I will also point out is that the cloud also provides new avenues for the attackers. So what we're actually seeing is malware that makes use of the cloud for elements of command and control, so whereas before you could look at your network traffic and say, you know, why are there strange connections to this other part of the world in the middle of the night, now, if you're looking at the traffic, all you'll see is connections to Gmail.

COMMISSIONER WESSEL: Your bilateral traffic. Right. Right.

MR. VILLENEUVE: We've seen malware that uses Google's encrypted Gtalk Chat as a mechanism of command and control. Cloud file share hosting services used as elements of command and control and also to drop exfiltrated data. So all of those things start obscuring any geographical indicators that we used to look at before.

COMMISSIONER WESSEL: Mr. Healey, any?

MR. HEALEY: Thank you.

Very briefly, it's just the latest in a long history of rushing ahead and then figuring out the security afterwards. Whether it was the Internet itself or almost every product that's ever come out, people have said, well, put this out and we'll figure out how to do it securely afterwards. So in that way, it's really not surprising.

And the cloud is doing this, which is wearing for espionage, but much more wearing for me is doing it also for industrial control systems, that we're taking these things that really break, things of steel and concrete, that you can't just reboot and replace, that when they break, people will die, and that we're saying, wait, let's connect that to the Internet.

And I understand, it's great economic reasons for doing it, but it needs to worry us very deeply.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR WORTZEL: Commissioner Fiedler.

HEARING CO-CHAIR FIEDLER: Mr. Bejtlich, you talked about communications companies being 23 percent of the target. You're talking about manufacturers. You're talking about IP providers. I'm trying to get at two things. I mean stealing technology is one thing. Everybody is stealing everything.

MR. BEJTLICH: Right.

HEARING CO-CHAIR FIEDLER: Listening or scooping up communications within the United States is another. How extensive do you believe Chinese interception of communications, public regular communications that all of us deal

with daily, is going on?

MR. BEJTLICH: So the cases that I talked about are the hardware and software manufacturers, and as far as we haven't seen any evidence of Chinese collection against American targets using that sort of thing.

HEARING CO-CHAIR FIEDLER: If we can do it all over the world, why can't they? And why aren't we talking about that?

MR. BEJTLICH: Well, so putting on my intel hat for a second, I would imagine that they would be pursuing the same sorts of systems that we have over time--satellite-based systems and that sort of thing.

We see them taking the technology from these telecom companies to improve their own capabilities and then also to come out with low-cost competitors who can then outbid everyone else on these sorts of national infrastructure projects.

HEARING CO-CHAIR FIEDLER: And are we seeing the adaptation, if you will, of hardware by Chinese manufacturers that allows them to do anything nefarious in the United States?

MR. BEJTLICH: I'm not personally aware of anything like that although--

HEARING CO-CHAIR FIEDLER: Anybody?

MR. BEJTLICH: --just on a quick point about that, we do see them trying to allay people's fears by saying, well, we'll have national certification and testing and this and that.

The problem is if any of these systems are remotely upgradable, and everything is, because you need to apply security patches, they'll test everything, they'll say it's clean. As soon as they ship it, and they need to upgrade it, that's when they'll slip in the back doors.

So I would caution anyone who thinks that the testing is--

HEARING CO-CHAIR FIEDLER: So it's a perpetual problem?

MR. BEJTLICH: Oh, absolutely, if it is possible to modify the device remotely.

HEARING CO-CHAIR FIEDLER: That's what the General was referring to about change--

MR. BEJTLICH: Yes.

HEARING CO-CHAIR FIEDLER: --and plugging this and plugging that in.

It also sounds to me, as a layman, that we're talking about what is essentially an indefensible problem. I mean we're doing this for years; we don't have a defense. We don't have an effective defense. The private sector doesn't have an effective defense. The defense establishment doesn't have an effective defense. This is a problem.

MR. BEJTLICH: It is, but it's interesting to me that it now resembles the real world. None of us came here in a tank. None of us put our kids to school

in Kevlar vests and helmets. We've developed ways to deal with an inherently vulnerable person biology system.

And we're there now with computers. It's been a fiction over time to think that we could defend computers in a way that we couldn't defend anything else, I think.

HEARING CO-CHAIR FIEDLER: Well, so let's get to that for a second. I mean are you saying that it's indefensible ultimately?

MR. BEJTLICH: If you are dealing with a professional intruder, the professional intruder will win. There's an inherent advantage to offense in cyber, I believe.

MR. HEALEY: The best that we can do is make it more difficult for them. You know, just like conflict in any other domain, it's going to be one force acting on another one, and this continual campaign, as Nart just discussed.

So the more things that we can do to make it more difficult for them, force them into other places, increase their work factor, make them give up, then that's the best that we can do, and if you look at the kinds of things that Mandiant does or other people come out with, most of these intrusions are not difficult.

They're able to use very simple--they don't have to be advanced. They don't even have to be that persistent, and the more that we force them to be advanced and persistent, the better off we'll be.

HEARING CO-CHAIR FIEDLER: Thank you.

We're going to break for a moment--

HEARING CO-CHAIR WORTZEL: We're going to break now.

HEARING CO-CHAIR FIEDLER: --gentlemen, and we'll call you back in after--

HEARING CO-CHAIR WORTZEL: We'll call you back in. We've got more questions.

HEARING CO-CHAIR FIEDLER: We've got a lot more questions.

HEARING CO-CHAIR WORTZEL: We got a lot of Commissioners that have more questions for you. Thank you.

Congressman Frank Wolf is the Representative for Virginia's 10th Congressional District, serving in Congress since 1981. He's also Chairman of the House Appropriations Subcommittee on Commerce-Justice-Science and Related Agencies; co-chair of the Tom Lantos Human Rights Commission; and a member of our sister commission, the Congressional-Executive Commission on China.

Chairman Wolf has also been a leader of congressional efforts to address cyber security concerns related to China. In 2006, congressional computers that contained information about political dissidents from around the world were compromised by people working from within China, including computers in Congressman Wolf's office.

In addition to working to raise awareness of cyber threats, the Congressman authored a number of cyber security provisions as part of the spending bill that funds the Departments of Commerce and Justice, NASA, and the National Science Foundation for FY 2012.

Some of these include: a Joint Cyber Security Center for Federal Civilian Agencies; new statutory certification requirements of IT systems to ensure supply chain security; expansion of training for FBI cyber agents; increased funding and resources for the FBI's unique cyber-related authorities and expertise; and requiring the FBI to produce an annual National Cyber Threat Assessment.

Congressman, the Commission is very pleased to have you here and to have your support. The nation is fortunate to have you as a leader in Congress. We're honored by your presence and look forward to your testimony.

STATEMENT OF FRANK WOLF
A U.S. REPRESENTATIVE FROM THE STATE OF VIRGINIA

MR. WOLF: Well, thank you very much, and I appreciate the opportunity to testify.

At the outset, I don't know if you saw today's--on the Internet--the Washington Post, Associated Press update, Monday, March 26, 5:21 a.m., out of Australia. It says Australia has banned Chinese technology giant Huawei from bidding to help build a nationwide high-speed Internet network due to concerns about cyber attacks traced to China.

Australian Prime Minister Julia Gillard said Monday the move was among, quote, "prudent decisions" to ensure that the planned network functions properly. The ban highlights concern about Beijing's cyber warfare efforts, a spate of hacking attempts aimed at Western companies and the role of Chinese equipment providers, which are expanding abroad.

So it's interesting that this story came out the very day that you have the hearing.

I want to thank you for the opportunity to testify today on this very important issue, and I appreciate more than I can tell you the continued good work by the Commission and your holding this field hearing in Manassas.

As you know, northern Virginia was really the birthplace of the Internet in the 1980s and '90s and remains the East Coast "high tech" hub today.

Today, northern Virginia is one of the frontlines in the emerging cybersecurity challenge, with a significant cyber workforce that is supporting U.S. defense and civilian agencies.

I have been deeply concerned about the cyber threat from China for nearly a decade. When I first started raising these concerns, the general attitude of the U.S. government was to keep everything secret or, in some cases, just to ignore the threat. In fact, when the Chinese attacked four of my office computers in 2006, along with many other House offices--I think there were about 17 members if I remember--I remember Congressman Kirk was one; Congressman Chris Smith was one--the FBI and others urged me not to disclose it publicly.

After nearly two years of waiting, I took to the House floor in June of 2008 to inform my colleagues, and the American people, about the incident and warn of the growing threat to the U.S. government and businesses.

I believed it was important for the public to better understand this threat and what the attackers wanted, not national security secrets, but information about Chinese dissidents that I had worked for.

The attacker first hacked into the computer of my foreign policy and human rights staff person, then the computers of my chief of staff, my legislative director and my judiciary staff person. On these computers was information

about all of the casework we have done on behalf of political dissidents and human rights activists around the world.

The computers, as I said, in other offices, including the House Foreign Affairs Committee, were also compromised.

It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress to help people who are suffering around the world was also open to view from these official computers.

In subsequent meetings with the FBI officials, it was revealed that the outside sources responsible for this attack came from within the People's Republic of China. These cyber attacks permitted the source to probe our computers to evaluate our system's defenses and to view and copy information. My suspicion is that I was targeted and the other members, like Congressman Chris Smith and Senator Kirk, by Chinese sources because of our history of speaking out about the Chinese government's abysmal human rights record.

I have spent hours with countless Chinese dissidents, ranging from Uyghur Muslim activist Rebiya Kadeer, to house church pastor and advocate Bob Fu, to former laogai prisoner, Harry Wu.

Just recently, I visited with an impressive group of Chinese lawyers in Washington for the National Prayer Breakfast. To a person, each loved their country and were rightly proud of their heritage, but all sought fundamental change. They longed to live in a land where they could worship freely, speak openly and enjoy the basic protections of a constitution grounded in rule of law. Their quarrel, and mine, is with a thin layer of leadership at the helm of the Chinese Communist Party that rules by fear and oppression.

Keep in mind Liu Xiaobo, the 2010 Nobel Prize winner, was not even permitted to leave his prison cell to go to Oslo, nor was his wife allowed to leave their residence. She was under house arrest.

Since I spoke out in 2008, there has been a sea change in how senior defense and intelligence officials are publicly discussing the cyber threat. Four years ago, some of these same leaders who were warning against even publicly acknowledging cyber attacks, much less the source of the threats, are now publicly warning of the threat in very stark terms.

I believe that this change has come about because these senior officials have determined that the situation has become so dangerous, as our networks and technology and companies become so interconnected, that they understand that public awareness is increasingly critical to deal with this threat.

For example, last month, during the appearance before the Senate Select Committee on Intelligence, FBI Director Robert Mueller said that while terrorism is the greatest threat today, quote, "down the road, the cyber threat will be the number one threat to the country."

2010 Pentagon report found, quote: "In the case of key national

security technologies, controlled equipment and other materials not readily obtainable through commercial means or academia, the People's Republic of China resorts to more focused efforts, including the use of its intelligence services and other-than-legal means, in violation of U.S. laws and export controls."

The report also highlighted China's cyber espionage efforts. The U.S. intelligence community notes that China's attempts to penetrate U.S. agencies are the most aggressive of all foreign intelligence organizations--far greater than the KGB ever was during the days of communism in the Soviet Union and during the '70s and '80s, and in many other areas, too.

Other senior U.S. military and intelligence officials have become increasingly vocal about their concerns about the scope of Chinese espionage and cyber attacks. Defense Intelligence Agency Chief General Ron Burgess also recently testified that--quote--he said: "China has used its intelligence services to gather information via a significant network of agents and contacts using a variety of methods. In recent years, multiple cases of economic espionage and theft of dual-use and military technology have uncovered pervasive Chinese collection efforts."

Last year, the usually reticent Office of the National Counterintelligence Executive issued a warning that, quote, "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The Counterintelligence Office took this rare step of singling out the Chinese due to the severity of the threats to the U.S. national and economic security.

And a March 8, 2012, Washington Post article described how, quote: "For a decade or more, Chinese military officials have talked about conducting warfare in cyberspace, but in recent years, they have progressed to testing attack capabilities during exercises. The PLA"--the People's Liberation Army--"probably would target transportation and logistics networks before an actual conflict to try to delay or disrupt the United States' ability to fight, according to the report prepared by Northrop Grumman"--for this Commission, and I want to commend the Commission and thank the Commission for requesting and publishing this important research.

We are beginning to witness the consequences of the cyber threat. According to a March 13, 2012, New York Times article, quote:

"During the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories, and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago."

In an interview with the New York Times, Homeland Security Secretary Janet Napolitano said, quote:

"I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was

looming. The information on a cyber attack is at the same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

Notably, Chinese espionage isn't limited to government agencies. In an October 4, 2011, Washington Post article, Chairman Mike Rogers remarked, quote:

"When you talk to these companies behind closed doors, they describe attacks that originate in China and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity."

Cyber espionage is having a real and corrosive effect on job creation, creating and causing jobs. You're taking jobs away from America, and last year, the Washington Post reported that, quote:

"The head of the military's U.S. Cyber Command, General Keith Alexander, said one U.S. company recently lost $1 billion--$1 billion--worth of intellectual property over the course of a couple of days--technology that they worked on for 20 plus years stolen by one adversary."

The record is clear: what policymakers used to reticently refer to as, quote, the "Advanced Persistent Threat" is now increasingly acknowledged as China's asymmetric warfare and economic strategy against our country, against America.

Because of our past reluctance to acknowledge the severity of this issue, the Congress and the administration are now struggling to keep up. As many are aware, several comprehensive cybersecurity bills have stalled in the Senate amid jurisdictional and partisan wrangling.

The House is quietly trying to advance more targeted bills, and I want to commend and thank my colleagues, Mike Rogers, chairman of the Intelligence Committee, and also Dutch Ruppersberger, the Democratic--the Ranking Member, and Peter King, chairman of the Homeland Security Committee, for their excellent leadership on this issue.

As chairman of the House Appropriations Subcommittee that funds the FBI, Commerce and National Institute for Standards and Technology, my subcommittee has also been funding some of the key civilian and law enforcement agencies involved in the fight against cyber threat.

That is why I prioritized cyber security programs in Fiscal Year 2012 Commerce-Justice-Science Appropriations bill, including significant increases in the FBI's joint cyber task force and requiring each agency to vet its IT equipment purchases. I also directed the FBI to produce an annual unclassified cyber report.

I am planning to take even more significant steps in the Fiscal Year 2013 bill that is currently under development, including--I want to tell this panel--adopting many of this Commission's recommendations. Your recommendations will not go unrecognized or ignored. We are going to adopt them, and we're going

to put them into law.

Although the government and the private sector have finally come to appreciate this threat and start to take the necessary steps to address it, the threat is evolving, and I am concerned that we may continue to be behind the curve.

One issue that the U.S. has failed to develop a coherent and strategic policy to address is the unique and unprecedented threat from Chinese state-owned and state-directed companies that are operating in the U.S. I believe this threat is particularly pronounced in Chinese telecom firms.

Earlier this year, The Economist magazine published a special report on Communist Party management of Chinese corporations. The article noted the Chinese government's particular support for its telecom and IT industry, noting that, quote, "the end result is the creation of a new class of a state companies: national champions that may not be owned by governments but are nevertheless closely linked to them."

The article reported that "the Communist Party has cells"--and that's a quote--"cells in most companies, in the private as well as state-owned sector--complete with their own offices and files on employees. It holds meetings that shadow formal board meetings and often trump their decisions."

According to The Economist, the Chinese government even has an expression for this strategy, quote: "The state advances while the private sector retreats."

Author Richard McGregor wrote that the executives at major Chinese companies have a, quote, "red machine" with an encrypted line to Beijing next to their Bloomberg terminals and personal items on their desks.

Given this level of party control in China's private sector, we shouldn't be surprised to learn that the PLA has been operating cyber militias out of telecom companies.

Last year, The Financial Times reported that the PLA has even documented how it will use telecom firms for foreign espionage and cyber attacks.

A paper published in the Chinese Academy of Military Sciences' journal noted, quote:

"These cyber militia should preferably be set up in the telecom sector, in the electronics and internet industries, and in institutions of scientific research," and its tasks should include, quote, "stealing, changing and erasing data" on enemy networks and their intrusion with the goal of "deception, jamming, disruption, throttling, and paralysis."

The same article also documented the growing number of PLA-led cyber militias housed in "private"--private--Chinese telecom firms.

The article reported on one example at the firm Nanhao: "Many of its

500 employees in Hengshui, just southwest of Beijing, have a second job. Since 2005, Nanhao has been home to a cyber militia unit organized by the People's Liberation Army. The Nanhao operation is one of thousands set up by the Chinese military over the past decade in technology companies and universities around the country. These units form the backbone of the country's Internet warfare forces, increasingly seen as a serious threat at a time of escalating global cybertensions."

This is what makes me so concerned about Chinese telecom firms' growing operations in the U.S. market. Chinese state-directed firms are collaborating and cooperating with the Chinese government to a degree that would be unfathomable in the U.S. or other Western countries.

And as these Chinese state-backed firms enter the U.S. market, it is unclear whether they will be playing by our rules or their own.

Currently, the most concerning of these Chinese telecoms is Huawei--and I read this report today, which you'll see later--which is attempting to increase its market share in the United States and around the world. Numerous government reports have linked Huawei's corporate leadership to the Chinese intelligence services and the People's Liberation Army, raising concerns about Huawei's networks and devices being subject to espionage by the Chinese government.

These connections are particularly noteworthy given Huawei's rapid rise as a telecom giant. According to a March 18 article in the Wall Street Journal, quote: "Huawei Technologies Company has almost doubled its workforce over the past five years as it strives to become a mobile technology heavyweight."

The article also notes that Huawei's network business has thrived at the expense of struggling Western network companies such as Alcatel-Lucent and Nokia Siemens Networks. Initially, Huawei supplied low-cost phones to telecommunications operations in the West under their own brand, but over the past year, Huawei has been quietly building and investing in its own brand of high-end smartphones and tablets.

Huawei executives make no secret of their goal to dominate the telecom market. In a March 6, 2012 interview with the technology news Web site, Engadget, Huawei device chief Richard Yu said, quote: "In three years we want Huawei to be the industry's top brand."

However, Huawei's growth in the U.S. market should give all Americans serious pause. Last week, respected national security reporter Bill Gertz wrote in The Washington Free Beacon about this Commission's recently released cybersecurity report.

Gertz wrote, quote: "New information about Chinese civilian telecommunications companies' close support of the Chinese military and information warfare programs is raising fresh concerns about the companies'

access to U.S. markets, according to a report by the Congressional U.S.-China Economic and Security Review Commission."

"One of the companies identified in the report as linked to the PLA is Huawei Technologies, a global network hardware manufacturer that has twice been blocked by the U.S. government since 2008 from trying to buy into U.S. telecommunications firms."

Gertz continued, quote: "Huawei is a well-established supplier of specialized telecommunications equipment, training and related technology to the PLA that has, along with others such as ZTE and Datang, received direct funding for R&D on the C4ISR. That's the high-tech intelligence collection systems capabilities."

The report further adds: "All these Chinese telecom firms originated as state research institutes and continue to receive preferential funding and support of the PLA."

Huawei's efforts to sell telecom equipment to U.S. networks has long troubled the U.S. defense and intelligence communities, which has been concerned that Huawei's equipment could easily be compromised and used in Chinese cyber attacks against the U.S. or to intercept phone calls and e-mails from the American telecom networks.

According to a 2005 report by the RAND Corporation, quote, "both the Chinese government and the military tout Huawei as a national champion, and one does not need to dig too deeply to discover that many Chinese information technology and telecommunications firms are the public face for, sprang from, or are significantly engaged in joint research with state research institutes under the Ministry of Information Industry, defense-industrial corporations, and the military.

In fact, the Washington Post reported that the National Security Agency called AT&T because of fears that China's intelligence agencies could insert digital trapdoors into Huawei's technology that would serve as secret listening posts in the U.S. communications network.

Over the last several years, Huawei's top executives' deep connections to the PLA and Chinese intelligence have been well documented. As Gertz summarized in his article, quote:

"A U.S. intelligence report produced last fall stated that Huawei Technologies was linked to the Ministry of State Security, specifically through Huawei's chairwoman, Sun Yafang, who worked for the Ministry of State Security, MSS, Communications Department before joining the company."

That is why senior administration officials in the Bush and the Obama administrations have repeatedly intervened to block Huawei's access to U.S. networks.

"In 2008, the Treasury Department-led Committee on Foreign

Investment in the United States, CFIUS, blocked Huawei from purchasing the U.S. telecommunications firm 3Com due to the company's links to the Chinese military," Gertz reported.

"Last year, under pressure from the U.S. government, Huawei abandoned their efforts to purchase the U.S. server technology company 3Leaf. In 2010, Congress opposed Huawei's proposal to supply mobile telecommunications gear to Sprint over concerns that Sprint was a major supplier to the U.S. military and intelligence agencies."

And I would say this: when the White House, the intelligence community, the Defense Department, and the Commerce Department--we had Secretary Bryson before us last week--all have worked to block Huawei from gaining access to U.S. networks, the American people should really take notice.

In all my years in Washington, very rarely have I seen defense, intelligence and civilian agencies come together in such a quiet but concerted effort to warn of a security threat from a foreign entity.

It is not just Huawei's longstanding and tight connections to Chinese intelligence that should trouble us. Huawei has also been a leading supplier of critical telecom services to some of the worst regimes around the world. Last year, the Wall Street Journal reported that Huawei, quote, "now dominates Iran's government-controlled mobile-phone industry." Iran. Everyone is concerned about Iran getting a nuclear weapon. You cannot not turn on the news and hear this. "It plays a role in enabling Iran's state security network."

You know what the state security network does to the Iranian people? And they're cooperating and helping.

Gertz reported that Huawei has also been "linked to sanctions-busting in Saddam Hussein's Iraq during the 1990s when that company helped network Iraqi air defenses at a time when U.S. and allied jets were flying patrols to enforce the no-fly zone." They were helping the Iraqis. They were helping Saddam.

I mean that, I mean they now--well, I won't go off on another--but I mean that should really get people very concerned. The company also worked with the Taliban during its short reign in Afghanistan to install a phone system in Kabul. Almost 200 people from my district died in the attack on the World Trade Center.

Now, everyone knew bin Laden lived in Sudan from '91 to '94. When he left and went there, they knew the connection. Everyone knew the connection. If you were deaf, maybe you didn't know it, or if you weren't following it, you didn't know it, but everyone knew the connection with the Taliban. Mullah Omar never sent bin Laden out and allowed him to stay, and they put a telephone system in for the Taliban. That should have everyone concerned. That should have--have you been up to the World Trade Center?

Given all this information, there should have been no doubt that Huawei poses--and how does somebody represent Huawei? I understand they just hired a former member of Congress to now---how do you do that? That's like the Simon and Garfunkel song "The Boxer." Remember that song, "A man hears what he wants to hear and disregards the rest."

How do you disregard that and come and register and lobby for a company that has been involved like this? Given all this information, there should be no doubt Huawei poses serious national and economic security threat to the U.S. It is no secret that the People's Republic of China has developed the most aggressive espionage operations in modern history, especially given its focus on cyber attacks and cyber espionage.

Perhaps that is why Beijing has ensured that Huawei is able to continue its global market growth by unsustainably low prices and Chinese government export assistance, according to this Commission's January 2011 report on the national security implications of Chinese telecom companies.

Due to China's secrecy, the full extent of Huawei's subsidies are not fully known, but given its unrealistically low prices, it remains unknown whether Huawei is even making a profit as it seeks to dominate the telecom market.

Why would the Chinese government be willing to generously subsidize such unprofitable products?

The American people have a right to know whether their government is doing everything it can to protect their cell phone and data networks. But I fear that with Huawei's rapid growth in the U.S. market, we may soon find that we are too intertwined with Huawei network equipment and devices to address potential security concerns. We must resolve these concerns before Chinese telecom firms make significant inroads on U.S. networks and not after.

As Huawei increases its lobbying presence in Washington every congressional office should know when they come in their connection to the Iranian issue, their connection to the Iraqi issue, their connection to the Taliban. We did a piece in the Congressional Record a week ago. We're sending it to every member of the House so they can't say, well, I didn't know, so they all know.

And as Huawei increases lobbying presence in Washington, members should be fully aware of the firm's intimate links to the PLA and the serious concerns of our defense and intelligence community.

Verizon, Sprint, AT&T, T-Mobile and other networks should not be selling Huawei devices given these security concerns. But if they do, they have an obligation to inform their customers of these threats. This is especially important when carriers are selling Huawei phones and tablets to corporate customers. They have a right to know that Beijing may be listening.

I want to thank you again for the opportunity to testify, and I look forward to working with the Commission on these issues, and, frankly, if the

Commission wasn't looking at some of these issues, I'm not so sure that anybody else would, and I want the Commissioners to know that your work has not been in vain.

We are going to take a lot of this and we're going to use it, and we're going to discuss it on the floor. It's going to be in the bill so it's not just like, it's not a resolution, it's going to be a law that we're going to come and push. With that, I thank you very much.

PREPARED STATEMENT OF FRANK WOLF
A U.S. REPRESENTATIVE FROM THE STATE OF VIRGINIA

Thank you for the opportunity to testify today on this very important issue. I appreciate the continued good work by the commission and your holding this field hearing here in Manassas. As you know, northern Virginia was really the birthplace of the Internet in the 1980s and 1990s and remains the East Coast "high tech" hub today.

Today, northern Virginia is one of the frontlines in the emerging cybersecurity challenge, with a significant cyber workforce that is supporting U.S. defense and civilian agencies.

I have been deeply concerned about the cyber threat from China for nearly a decade. When I first started raising these concerns, the general attitude of the U.S. government was to keep everything secret – or in some cases – just to ignore the threat. In fact, when the Chinese attacked four of my office computers in 2006, along with many other House offices and committees, the FBI and others urged me not to disclose it publicly.

After nearly two years of waiting, I took to the House floor in June 2008 to inform my colleagues – and the American people – about the incident and warn of the growing threat to the U.S. government and businesses.

I believed it was important for the public to better understand this threat and what the attackers wanted – not national security secrets, but information about Chinese dissidents with whom I had had worked.

The attacker first hacked into the computer of my foreign policy and human rights staff person, then the computers of my chief of staff, my legislative director, and my judiciary staff person. On these computers was information about all of the casework I have done on behalf of political dissidents and human rights activists around the world.

The computers in the offices of several other Members were similarly compromised, as well as a major committee of the House, the Foreign Affairs Committee.

It is logical to assume that critical and sensitive information about U.S. foreign policy and the work of Congress to help people who are suffering around the world was also open to view from these official computers.

In subsequent meetings with FBI officials, it was revealed that the outside sources responsible for this attack came from within the People's Republic of China. These cyber attacks permitted the source to probe our computers to evaluate our system's defenses and to view and copy information. My suspicion is that I was targeted by Chinese sources because of my long history of speaking out about the Chinese government's abysmal human rights record.

I have spent hours with countless Chinese dissidents ranging from Uyghur Muslim activist Rebiya Kadeer, to house church pastor and advocate Bob Fu, to former laogai prisoner Harry Wu.

Just recently I visited with an impressive group of Chinese lawyers in Washington for the National Prayer Breakfast. To a person, each loved their country and where rightly proud of their heritage. But all sought fundamental change. They longed to live in a land where they could worship freely, speak openly and enjoy the basic protections of a constitution grounded in rule of law. Their quarrel – and mine – is with a thin layer of leadership at the helm of the Chinese communist party that rules by fear and oppression.

Since I spoke out in 2008, there has been a "sea change" in how senior defense and intelligence officials are publicly discussing to the cyber threat. Four years ago, some of these same leaders who were warning against even publicly acknowledging cyber attacks – much less the source of the threat – are now publicly warning of the threat in very stark terms.

I believe that this change has come about because these senior officials have determined that the situation has become so dangerous, as our networks and technology and companies become so interconnected, that they understand that public awareness is increasingly critical to dealing with this threat.

For example, last month during an appearance before the Senate Select Committee on Intelligence FBI Director Robert Mueller said that while terrorism is the greatest threat today, "down the road, the cyber threat will be the number one threat to the country."

A 2010 Pentagon report found "… [i]n the case of key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia, the Peoples Republic of China resorts to more focused efforts, including the use of its intelligence services and other-than legal means, in violation of U.S. laws and export controls."

The report also highlighted China's cyber-espionage efforts. The U.S. intelligence community notes that China's attempts to penetrate U.S. agencies are the most aggressive of all foreign intelligence organizations.

Other senior U.S. military and intelligence officials have become increasingly vocal about their concerns about the scope of Chinese espionage and cyberattacks. Defense Intelligence Agency chief General Ron Burgess also recently testified that "China has used its intelligence services to gather information via a significant network of agents and contacts using a variety of methods... In recent years, multiple cases of economic espionage and theft of dual-use and military technology have uncovered pervasive Chinese collection efforts."

Last year, the usually-reticent Office of the National Counterintelligence Executive issued a warning that "Chinese actors are the world's most active and persistent perpetrators of economic espionage." The counterintelligence office took this rare step of singling out the Chinese due to the severity of the threat to U.S. national and economic security.

And a March 8, 2012 Washington Post article described how "[f]or a decade or more, Chinese military

officials have talked about conducting warfare in cyberspace, but in recent years they have progressed to testing attack capabilities during exercises… The (PLA) probably would target transportation and logistics networks before an actual conflict to try to delay or disrupt the United States' ability to fight, according to the report prepared by Northrop Grumman" for this commission -- and I want to commend this commission for requesting and publishing this important research.

We are beginning to witness the consequences of the cyber threat. According to a March 13, 2012 New York Times article "[d]uring the five-month period between October and February, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories and databases, according to the Department of Homeland Security, compared with 11 over the same period a year ago."

In an interview with The New York Times, Homeland Security Secretary Janet Napolitano said "I think General Dempsey said it best when he said that prior to 9/11, there were all kinds of information out there that a catastrophic attack was looming. The information on a cyberattack is at the same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

Notably, Chinese espionage isn't limited to government agencies. In an October 4, 2011 Washington Post article, Chairman Mike Rogers remarked: "When you talk to these companies behind closed doors, they describe attacks that originate in China, and have a level of sophistication and are clearly supported by a level of resources that can only be a nation-state entity."

Cyberespionage is having a real and corrosive effect on job creation. Last year, the Washington Post reported that, "[t]he head of the military's U.S. Cyber Command, Gen. Keith Alexander, said that one U.S. company recently lost $1 billion worth of intellectual property over the course of a couple of days – 'technology that they'd worked on for 20-plus years – stolen by one of the adversaries.'"

The record is clear: what policymakers used to reticently refer to as the "Advanced Persistent Threat" is now increasingly acknowledged as China's asymmetric warfare and economic strategy against the U.S.

Because of our past reluctance to acknowledge the severity of this issue, the Congress and the administration are now struggling to keep up. As many are aware, several comprehensive cybersecurity bills are stalled in the Senate amid jurisdictional and partisan wrangling.

The House is quietly trying to advance more targeted bills and I want to commend my colleagues Mike Rogers, chairman of the Intelligence Committee, and Peter King, chairman of the Homeland Security Committee, for their excellent leadership on this issue.

As chairman of the House Appropriations subcommittee that funds the FBI, Commerce Department and the National Institute for Standards and Technology (NIST), my subcommittee has also been funding some of the key civilian and law enforcement agencies involved in the fight against the cyber threat.

That is why I prioritized cybersecurity programs in the fiscal year 2012 Commerce-Justice-Science

Appropriations bill, including significant increases to the FBI's joint cyber task force and requiring each agency to vet its IT equipment purchases. I also directed the FBI to produce an annual unclassified cyber report.

I am planning take even more significant steps in the fiscal year 2013 bill that is currently under development, including adopting many of this commission's recommendations.

Although the government and the private sector have finally come to appreciate this threat and start to take the necessary steps to address it, the threat is evolving and I am concerned that we may continue to be behind the curve.

One issue that the U.S. has failed to develop a coherent and strategic policy to address is the unique and unprecedented threat from Chinese state-owned or state-directed companies that are operating in the U.S. I believe this threat is particularly pronounced from Chinese telecom firms.

Earlier this year, The Economist magazine published a special report on Communist Party management of Chinese corporations. The article noted the Chinese government's particular support for its telecom and IT industry noting that, "the end result is the creation of a new class of state companies: national champions that may not be owned by governments but are nevertheless closely linked to them"

The article reported that "[t]he (Communist) party has cells in most big companies – in the private as well as state-owned sector – complete with their own offices and files on employees. It holds meetings that shadow formal board meetings and often trump their decisions"

According to The Economist, the Chinese government even has an expression for this strategy: "The state advances while the private sector retreats."

Author Richard McGregor wrote that the executives at major Chinese companies have a "red machine" with an encrypted line to Beijing next to their Bloomberg terminals and personal items on their desks.

Given this level of party control in China's private sector, we shouldn't be surprised to learn that the PLA has been operating cybermilitias out of telecom companies.

Last year, The Financial Times reported that the PLA has even documented how it will use telecom firms for foreign espionage and cyberattacks.

A paper published in the Chinese Academy of Military Sciences' journal noted: "[These cyber militia] should preferably be set up in the telecom sector, in the electronics and internet industries and in institutions of scientific research," and its tasks should include "stealing, changing and erasing data" on enemy networks and their intrusion with the goal of "deception, jamming, disruption, throttling and paralysis."

The same article also documented the growing number PLA-led cyber militias housed in "private" Chinese telecom firms.

The article reported on one example at the firm Nanhao [Nan-how]: "many of its 500 employees in Hengshui [Hang-shoo], just south-west of Beijing, have a second job. Since 2005 Nanhao has been home to a cybermilitia unit organized by the People's Liberation Army. The Nanhao operation is one of thousands set up by the Chinese military over the past decade in technology companies and universities around the country. These units form the backbone of the country's internet warfare forces, increasingly seen as a serious threat at a time of escalating global cybertensions."

That is what makes me so concerned about Chinese telecom firms' growing operations in the U.S. market. Chinese state-directed are collaborating and cooperating with the Chinese government to a degree that would be unfathomable in the U.S. or other Western economies.

And as those Chinese state-backed firms enter the U.S. market, it is unclear whether they will be playing by our rules, or their own.

Currently, the most concerning of these Chinese telecoms is Huawei, which is attempting to increase its market share in the United States and around the world. Numerous government reports have linked Huawei's corporate leadership to the Chinese intelligence services and the People's Liberation Army (PLA), raising concerns about Huawei networks and devices being subject to espionage by the Chinese government.

These connections are particularly noteworthy given Huawei's rapid rise as a telecom giant. According to a March 18 article in the Wall Street Journal, "Huawei Technologies Co. has almost doubled its work force over the past five years as it strives to become a mobile technology heavyweight."

The article also noted that "Huawei's network business has thrived at the expense of struggling Western network companies such as Alcatel-Lucent Co. and Nokia Siemens Networks. Initially, Huawei supplied low-cost phones to telecommunications operators in the West under their own brand, but over the past year, Huawei has also been quietly building and investing in its own brand of high-end smartphones and tablets."

Huawei executives make no secret of their goal to dominate the telecom market. In a March 6, 2012, interview with the technology news Web site, Engadget, Huawei device chief Richard Yu said "[i]n three years we want Huawei to be the industry's top brand."

However, Huawei's growth in the U.S. market should give all Americans serious pause. Last week, respected national security reporter Bill Gertz wrote in The Washington Free Beacon about this commission's recently released cybersecurity report.

Gertz wrote: "[n]ew information about Chinese civilian telecommunications companies' close support of the Chinese military and information warfare programs is raising fresh concerns about the companies' access to U.S. markets, according to a report by the congressional US-China Economic and Security Review Commission."

"One of the companies identified in the report as linked to the PLA is Huawei Technologies, a global network hardware manufacturer that has twice been blocked by the U.S. government since 2008 from trying to buy into U.S. telecommunications firms," Gertz continued. "Huawei is a well established supplier of specialized telecommunications equipment, training and related technology to the PLA that has, along with others such as Zhongxing, and Datang, received direct funding for R&D on C4ISR [high-tech intelligence collection] systems capabilities."

The report further added, "[a]ll of these [Chinese telecom] firms originated as state research institutes and continue to receive preferential funding and support from the PLA."

Huawei's efforts to sell telecom equipment to U.S. networks have long troubled the U.S. defense and intelligence community, which has been concerned that Huawei's equipment could be easily compromised and used in Chinese cyberattacks against the U.S. or to intercept phone calls and e-mails from American telecom networks.

According to a 2005 report by the RAND Corporation, "both the [Chinese] government and the military tout Huawei as a national champion," and "one does not need to dig too deeply to discover that [many Chinese information technology and telecommunications firms] are the public face for, sprang from, or are significantly engaged in joint research with state research institutes under the Ministry of Information Industry, defense-industrial corporations, or the military."

In fact, in 2009, The Washington Post reported that the National Security Agency "called AT&T because of fears that China's intelligence agencies could insert digital trapdoors into Huawei's technology that would serve as secret listening posts in the U.S. communications network.

Over the last several years, Huawei's top executives' deep connections to the PLA and Chinese intelligence have been well documented. As Gertz summarized in his article, "a U.S. intelligence report produced last fall stated that Huawei Technologies was linked to the Ministry of State Security, specifically through Huawei's chairwoman, Sun Yafang, who worked for the Ministry of State Security (MSS) Communications Department before joining the company."

That is why senior administration officials in the Bush and Obama administrations have repeatedly intervened to block Huawei's access to U.S. networks. "In 2008, the Treasury Department-led Committee on Foreign Investment in the United States (CFIUS) blocked Huawei from purchasing the U.S. telecommunications firm 3Com due to the company's links to the Chinese military," Gertz reported.

"Last year, under pressure from the U.S. government, Huawei abandoned their efforts to purchase the U.S. server technology company 3Leaf. In 2010, Congress opposed Huawei's proposal to supply mobile telecommunications gear to Sprint over concerns that Sprint was a major supplier to the U.S. military and intelligence agencies."

When the White House, Intelligence Community, Defense Department and the Commerce Department all have worked to block Huawei from gaining greater access to U.S. networks, the American people

should take notice.

In all my years in Washington, very rarely have I seen the defense, intelligence and civilian agencies come together in such a quiet but concerted effort to warn of a security threat from a foreign entity.

It's not just Huawei's longstanding and tight connections to Chinese intelligence that should trouble us. Huawei has also been a leading supplier of critical telecom services to some of the worst regimes around the world. Last year, the Wall Street Journal reported that Huawei "now dominates Iran's government-controlled mobile-phone industry…it plays a role in enabling Iran's state security network."

Gertz reported that Huawei has also been "linked to sanctions-busting in Saddam Hussein's Iraq during the 1990s, when the company helped network Iraqi air defenses at a time when U.S. and allied jets were flying patrols to enforce a no-fly zone. The company also worked with the Taliban during its short reign in Afghanistan to install a phone system in Kabul."

Given all of this information, there should be no doubt Huawei poses a serious national and economic security threat to the U.S. It is no secret that the Peoples Republic of China has developed the most aggressive espionage operation in modern history, especially given its focus on cyberattacks and cyberespionage.

Perhaps that is why Beijing has ensured that Huawei is able to continue its global market growth by "unsustainably low prices and [Chinese] government export assistance," according to this commission's January 2011 report on the national security implications of Chinese telecom companies.

Due to China's secrecy, the full extent of Huawei's subsidies are not fully known. But given its unrealistically low prices, it remains unknown whether Huawei is even making a profit as it seeks to dominate the telecom market. Why would the Chinese government be willing to generously subsidize such unprofitable products?

The American people have a right to know whether their government is doing everything it can to protect their cell phone and data networks.

But I fear that with Huawei's rapid growth in the U.S. market, we may soon find that we are too intertwined with Huawei network equipment and devices to address potential security concerns. We must resolve these concerns before Chinese telecom firms make significant inroads on U.S. networks, not after.

And as Huawei increases its lobbying presence in Washington, members should be fully aware of the firm's intimate links to the PLA and the serious concerns of our defense and intelligence community.

Verizon, Sprint, AT&T, T-Mobile and other U.S. network carriers should not be selling Huawei devices given these security concerns. But if they do, they have an obligation to inform their customers of these threats. This is especially important when carriers are selling Huawei phones and tablets to corporate customers. They have a right to know that Beijing may be listening.

Thank you again for the opportunity to testify this morning. I look forward to working with this commission as we continue to address this challenge.

HEARING CO-CHAIR WORTZEL: Thank you, Congressman Wolf.

MR. WOLF: Thank you so much.

HEARING CO-CHAIR WORTZEL: Do you have time for a couple of questions?

MR. WOLF: Sure, I do. Yes, sir.

HEARING CO-CHAIR WORTZEL: Commissioner Wessel.

COMMISSIONER WESSEL: Mr. Chairman, I actually don't have a question. I have more of a statement of thanks for all that you do. I'm a Democrat, as you know. This Commission has worked hard over all of our years. I think that each of the last five years, we've had a bipartisan unanimous report, and your leadership on these issues is deeply appreciated.

I know it hasn't been easy. You've taken on some big transactions. Each time you've done that, it's been validated by law enforcement and other officials in the government.

And as you just pointed out with the Washington Post article, Huawei is being banned from one of our major allies. I don't think there can be any question about Huawei's ties to the government, what they're trying to do to infiltrate our telecommunication system, and your persistence going at this. I think this is a great tribute to your work over the years and appreciated by the public for what you do.

MR. WOLF: Well, thank you very much.

COMMISSIONER WESSEL: Thank you.

MR. WOLF: And this is totally a bipartisan or a nonpartisan issue here.

COMMISSIONER WESSEL: Agree.

MR. WOLF: Yes. Thank you.

HEARING CO-CHAIR WORTZEL: Thank you.

Commissioner Fiedler.

HEARING CO-CHAIR FIEDLER: I would just like to say, Frank, that we know each other for 20 years, and today you've done again what you always do, which is you speak truth to power.

Thank you, again.

MR. WOLF: Thank you. Appreciate that.

HEARING CO-CHAIR WORTZEL: Thank you, sir.

MR. WOLF: Okay. Thank you very much.

HEARING CO-CHAIR WORTZEL: We're going to take a short five-minute break. I'll try and hold us to that time and then come right back with you three gentlemen.

[Whereupon, a short recess was taken.]

PANEL I – QUESTIONS AND ANSWERS (continued)

HEARING CO-CHAIR WORTZEL: Commissioner Cleveland will lead off with the next question.

COMMISSIONER CLEVELAND: Actually I was interested in your comment that it was 416 days on average before the breach was detected. Why does it take so long? And then what finally catches the attention of a company to address the issue?

MR. BEJTLICH: I'll answer the easier part. The easier part is the reason why people finally discover a problem has been third-party notification. 94 percent of the cases we worked someone had to come in and say you've got this problem.

COMMISSIONER CLEVELAND: And how did they know?

MR. BEJTLICH: Pardon?

COMMISSIONER CLEVELAND: And how did they know? What was the sequence?

MR. BEJTLICH: Many times the law enforcement agency, the intel agency, is working other cases, and they see activity that suddenly involves other companies, and they say, well, those companies are compromised as well, and so they sort of leapfrog. Just as the activity leapfrogs, the intel analysts leapfrog and say, all right, we now need to do notification of these other organizations.

COMMISSIONER CLEVELAND: So you're suggesting that most notifications in 94 percent of these cases do come from law enforcement or the government?

MR. BEJTLICH: Of the cases we worked, yes, they were, almost all of them were FBI. The FBI has been very good over the last five years in terms of telling people about this.

COMMISSIONER CLEVELAND: Interesting.

MR. BEJTLICH: This is a game changer because you can't ignore either that visit by an agent or that piece of paper with that FBI logo that says you have a serious problem, and if you can get into a cleared facility, we'll talk to you about what it is.

COMMISSIONER CLEVELAND: Interesting. Okay.

MR. BEJTLICH: You asked why it takes so long?

COMMISSIONER CLEVELAND: Right.

MR. BEJTLICH: I would say, believe it or not, many companies are simply not structured to deal with this. There is a perception that if you simply buy enough of the right technology, and you deploy enough of it, and the wall is high enough, then you're okay. And that is patently not true.

We've got teams now that--to give you an example, at General Electric it took me building a team of 40 people with a $10 million budget to even make a

dent in this problem, and it took several years to get to that capability, and I had to call in every favor and get every friend that I could to join me to try to fight these guys.

You cannot do that at every single one of these victims out there, and there are hundreds, if not thousands. So it is very difficult. Now, the top tier companies, top-end defense contractors, those sorts of people, can afford [it], and financials can afford this sort of thing. Almost everyone else, it's just well beyond their capability, and so that's why a lot of them have to turn to outside partners or something like that.

It is a wake-up call for a company to realize that all of these millions of dollars they've spent over the years have just made no dent against a dedicated intruder.

COMMISSIONER CLEVELAND: Okay. Are any of you aware of the Lieberman-Collins legislation on the Hill?

MR. BEJTLICH: Yes.

COMMISSIONER CLEVELAND: Again, I guess the question is for you. Do you think that, as it's characterized in a New York Times article, the greater authority to regulate the security used by companies that run the nation's infrastructure and establish and enforce minimum standards on companies whose service or products would lead to mass casualties, evacuations or major economic damage, do you think that that legislation squares with your kind of analysis of are we compromised rather than are we vulnerable?

MR. BEJTLICH: I don't oppose regulation. I fear that regulation that results in more paperwork is not going to be the right result. We've seen that with FISMA. FISMA has been pretty much an abject failure over the last ten years. Not that the law is written poorly, but the implementation was terrible. It just became a giant paperwork exercise.

If we spent more attention on the regulatory side saying “if you're a covered entity of critical infrastructure and maybe a publicly traded company, once a year”--I'd prefer more often, but say “once a year you should find if you are compromised.” That's the game changer. That takes it from being a reactive stance with the FBI visiting to a more proactive stance of regularly finding out if you have this problem.

Once you do that, you can tailor defenses based on what's found as opposed to going through sort of an academic exercise where you have a standard, are you compliant with the standard; it's more of an audit. I prefer it to be based on what's the score of the game as opposed to how tall the players are, where they went to college, how fast they can run the 40, those sorts of inputs.

COMMISSIONER CLEVELAND: Would the companies carry out this kind of audit themselves or do you think this is something that should be done by some

external public-private?

MR. BEJTLICH: I think it has to be--so that if the companies aren't capable of defending themselves, and most of them aren't, I think it would have to be done by a third party, maybe someone who is a certified assessor similar to what's done in PCI.

COMMISSIONER CLEVELAND: Okay. And General Cartwright urged a multilateral approach to this. What I haven't heard is two dimensions of it. The first is what do you think the European response would be to a more concerted effort to get ahead of this problem or at least catch up?

And second, would one of you choose to compare what the Chinese are accused of doing with, say, what the Russians are doing? Draw, differentiate it, if you will, the scope, the target, the management by the government. What's the--how would you distinguish between the Russian cyber espionage efforts and the Chinese? And then, the second question, the European?

That's the way you get in under your time.

[Laughter.]

MR. BEJTLICH: In the activity that we've seen, Chinese activity far exceeds [Russian activity]. And this isn't sort of us looking at just general reporting. This is our workload. The Chinese activity far exceeds the Russian activity.

We have certain playbooks that we can judge an actor by. When we see the Chinese, it's very obvious it's them. The Russians tend to be much more selective, creative. They tend to play by the rules of the Cold War.

When I did consulting and we found the Russians, when we pushed back on them, they would disappear for six months. They would show you some respect. They would not seek to stay present the way the Chinese do. The Chinese, you kick them out on Friday; they're coming back on Monday or maybe they're coming back on Sunday night. It's a completely different set of actors because they know that there's going to be a spokesman on TV on Monday morning saying we denounce hacking; we're a victim. The Russians, they don't act that way at all.

MR. HEALEY: Both do have unclear ties, though, between the government and non-state actors, and whether that's organized crime or companies or private hacking groups, that does confuse things, but, again, it only confuses things if we let it. We can still go government to government.

MR. VILLENEUVE: Yes. My challenge is sorting out attacks that are interesting from the general run-of-the-mill cyber crime activity that you see constantly. So when it comes to a few interesting cases involving what appears to be Russian cyber crime infrastructure, I've seen some infrastructure that's typically associated with malware associated with banking fraud, people that try to steal your credit card numbers and drain your bank account, being used for

activities that look more like espionage than it does cyber crime, and that is that these systems are usually designed specifically to steal banking-related information.

But we've seen some variants that have a secondary payload that sucks up all the documents on a computer, and it makes me wonder why is a gang or a cyber criminal outfit that's interested in bank accounts and credit card numbers stealing all of the documents, PowerPoints and Excel sheets [included], off the target's computer?

HEARING CO-CHAIR WORTZEL: Thank you very much.

Commissioner D'Amato.

COMMISSIONER CLEVELAND: Can they answer the European question?

COMMISSIONER D'AMATO: Thank you very much, Mr. Chairman. And I want to thank the panel for very interesting testimony and the dialogue here.

It is a very, very important area which cries out, in my opinion, for more effective U.S. government action. It seems to me that the whole structure of deterrence and penalties and incentives is inadequate to the problem here. We know what a deterrence is in the nuclear area. Obviously, if somebody is going to attack us, the Russians, for example, the nuclear field, they face unacceptable damage in return. We don't have any kind of unacceptable damage to the Chinese for this sort of behavior.

So, let me ask you just a couple of questions, and if you have some additional ideas after the hearing, we'd like to hear them as well in a follow-up.

But in terms of industry, what does industry need in the way of more incentives to come to the U.S. government for intercession? What kind of incentives can we provide industry to do that?

And, secondly, more difficult, is how can we develop a more systematic and effective structure of penalties when we find out after the disclosure who and what has been done to us?

What always comes to my mind is that, you know, we have to trade apples for oranges because you have not necessarily got apples for apples here. The thing that's the most important to the Chinese is access to the United States market. When you affect their access to the United States market, it gets their attention. That would be a penalty or a structure of penalties that might be available.

There may be other penalties that are available. Right now, we don't have effective deterrence. We don't have effective penalties, and we don't have effective incentives. Would you agree with that, and do you have any thoughts about how that can be more effectively improved?

MR. BEJTLICH: I can make a short comment. I have a feeling Jason has more to say about this. You used a phrase that I heard all the time when I was in private industry. Well, I'm still in private industry, but when I wasn't a service

provider--"access to markets." That is the number one concern of the American companies. They want to maintain access to the Chinese markets, and so what happens is they're willing to accept these outrageous technology transfer deals, these supposed safeguards that say, well, “we will not have uniformed PLA members on the contract with the American company; we will not have military intelligence officers on the contract with the company.”

It's clearly, it's silly, and yet the American companies are willing to make these deals because--I've heard this firsthand as well--if we don't get in there, then the French will, the Germans will, the Australians will. Of course, then the Chinese steal everything they need from them as well. So that argument is kind of bogus.

But that's me. Until we can get the top level of these companies believing that, no, they don't, the Chinese don't play fair, they will take everything they can from you through the tech transfer, and then they'll steal everything else that they need, I think that's where the first point--once you make that connection with the management that's making these business decisions, I think that would be a good start.

MR. HEALEY: Thank you for the question.

I do generally agree. First, briefly, on deterrence. I think deterrence is working if you're looking at just a narrow range of things. We haven't had the large-scale disruptive 9/11 kind of attack yet, and I think deterrence, you know, only Russia and China governments can really an attack that's significant and continue it on for the weeks or months--the campaign that Nart talked about.

So I think deterrence is good for that range of cyber conflicts because we haven't seen--there are many kinds of cyber conflicts that are possible. We've only seen a small subset of the possible range of cyber conflicts. So I think deterrence is useful for that part.

Your question asks some, a little bit about our face to China and some the government's face with the individual companies. I'll address each of those.

I do agree that there's a wide range of carrots and sticks that we could possibly use to influence Chinese behavior. We've heard just one this morning with what Australia did in saying we're not going to buy your stuff anymore. That usually doesn't get brought up in conversations within the government. Usually they're thinking about, well, we can attack them back, or, you know, a limited set of things.

I would really encourage the government to have a wider range of carrots and sticks. Normally, that's a role that think tanks and other people get involved with, you know, for what are our options with Iran; what are our options with Pakistan? We have daily events at the Atlantic Council on a discussion for that. We don't have that discussion here because everyone says I'm sorry, we can't have that conversation, it's classified.

It's absolutely bizarre to me that we're classifying ourselves into a place where we can't have a real conversation about our leverage.

And, second, when it's facing for the U.S. companies, there are some things that only the government can do, and that's why, as I mentioned in my testimony, I'd like the government to come out and put some pressure on China with carrots and sticks. I think there are some real facts that can get out.

This summer we were having a conversation with the Aspen Strategy Group, with Joe Nye and Madeleine Albright and others, to try and convince them. We had to use Nart's reports. We had to use Mike Gross's reporting in Vanity Fair and Ellen Nakashima articles. We had no facts from the government, only assertions that China was bad. I'd love to see more of that.

And, in general, I am not against regulation, but it needs to be regulation that increases the attacker's work factor much, much more than it does ours, and I don't have a lot of confidence that the regulation that would be implemented would do that. I'm afraid, like Rich pointed out, that it would be a paperwork exercise, that it would be a lot of make-work that doesn't necessarily help our security at all. It just makes bureaucrats feel better.

HEARING CO-CHAIR WORTZEL: Vice Chairman Reinsch.

VICE CHAIRMAN REINSCH: Thank you.

I was reflecting as you were talking that I haven't read the article about the Australians, but it occurs to me that one of the reasons the Australians could do what they did is because China hasn't signed the WTO Government Procurement Agreement so the Australians have no obligations to them.

Of course Australia's policy, as well as our policy, is to get the Chinese to sign because we want access to their market. So there are tradeoffs. China has no obligations to us either, which then goes back to what you were saying. My experience with the companies you're talking about, and I represent a lot of them, is I think you're right, that they are not at the top focused in the way you want them to be focused.

One of the reasons is they're making a lot of money, and that allows them to not think about this problem--sort of short-term versus long-term--but a different discussion.

I was going to ask you about the cloud, but Mike did that. Let me ask a related question. Thinking more about attacks designed to create disruptions rather than to try to obtain information, to what extent are our efforts here to promote interconnectedness of the electric grid or various other networks going to make that problem more difficult to solve should such an attack occur?

MR. BEJTLICH: I think it makes it exceptionally difficult. Consider all of the smart meters being put all over the country. These devices in many cases are being shipped such that they cannot be upgraded. In other words, if there's a vulnerability found, it's permanent, and the only way to fix it is to spend money,

some dollars, to replace them, and that's not going to happen. These things are on a ten-year refresh cycle, 15-20 year refresh cycle in some cases.

But yet they're going forward because in some ways it seems an environmental measure, it's a cost saving measure, it's a convenience measure, and that sort of thing. So it exposes a huge vulnerability.

VICE CHAIRMAN REINSCH: But it also means that there are costs to not doing it, which you've just enumerated.

MR. BEJTLICH: Yes.

VICE CHAIRMAN REINSCH: In terms of efficiencies and environment and so on.

MR. BEJTLICH: Right. Right.

VICE CHAIRMAN REINSCH: Anybody else want to comment on that? I've got another one.

MR. HEALEY: It's been interesting, as we've looked back at the history of cyber conflict, there are a couple of things that we've learned from that history. And in some way, they go against some of the myths that we have about things that are doable in cyber.

One, the large-scale conflicts have either been short-term and widely disruptive--think of Aurora, like a virus or a worm that hits, but it's gone a week later--or targeted and persistent, meaning they only affect a small amount of targets, and because it's a small amount of targets, you can keep it for a long time.

We have not seen something that was both wide scale and persistent over a long period of time. Now, because so much of cyber damage, you can just replace, you can replace the drives, you can reload your information, and you're back.

Connecting to the industrial control systems to the Internet is one of those things that can make that not true anymore where now you can create more permanent damage. So who might want to do that? When it's coming to hacktivists and nuisance groups, we've found there are lots of hackers that would be interested in trying to get into these systems, either because they're disgruntled or they've got too much Mountain Dew rolling around in their system, and they're bored at 2 a.m.

Some of the new hactivist groups could certainly want to do it to show their anger and rage over the issue that they might want, and that's possible, but again it would probably be more localized disruption and not widespread over a large area.

It really does come down to nation states, particularly Russia and China, that may, that have the capability and may some day have the intent to do such things. Fortunately, as was mentioned in the other one, they're the ones--that's the problem where deterrence is most helpful because they're unlikely to

want to do that outside of a real geopolitical crisis. It's not the kind of thing that's just going to happen on the first morning most likely, but, as Nart talked about, this system of campaigns that goes on for days and weeks.

It's frankly a myth at that level of cyber conflict that it's going to be speed of light. I was in the Air Force. A single dog fight might be over very quickly, but air campaigns would last weeks, months and years, and it is likely that cyber campaigns are going to be the same.

VICE CHAIRMAN REINSCH: I was in Houston last week giving a speech, and someone approached me afterwards to tell me her story about IP theft. They may be one of your customers, Mr. Bejtlich. I don't know. She didn't say. But it was a case involving hundreds of millions of dollars, if not a billion, of their IP, all of which had been stolen.

But the operative factor here was what the Chinese did was steal her employees. They got people who were working for her to leave and go work for basically a shell firm and they took with them a lot of information as well as access codes that allowed them to obtain further information.

How big a piece of the problem is that compared to what we've been talking about heretofore?

MR. BEJTLICH: I would say that's definitely an escalation. That's not something I've seen too often, but at any point where it escalates into a physical manifestation like that, that's pretty worrying.

MR. HEALEY: I would say that happens within China itself. I mean I was in Hong Kong with one of the major banks, and it was well-known that it was one of the reasons we didn't expand as much as we might have in China because you would have employees that would happily go over to some other company and take information. It wasn't just in banking. It was across all these informations. You didn't have that same kind of loyalty or feeling, those norms that you would in a U.S. company.

VICE CHAIRMAN REINSCH: Is there anything that you can do about that?

HEARING CO-CHAIR WORTZEL: Bill, I'm going to move on to the next Commissioner, and if there's time for a second round, we'll let you continue.

Commissioner Bartholomew.

COMMISSIONER BARTHOLOMEW: Thanks very much, and thank you, gentlemen, both for your testimony today and for the work that you've been doing, particularly your work that has had a huge impact in the public sector.

Mr. Villeneuve, I'd like to acknowledge really that I think it was a lot of the GhostNet work that broke a lot of this out into the public domain so that the debate is being carried on more fulsomely than perhaps it would have been otherwise. So thank you very much for that.

I think what I've heard from all of you is a need for more information

to be shared, that people be willing to admit when their systems have been hacked into or compromised so that people can learn how it's happening, what the targets are, and what potentially could be done.

I'm interested particularly when it comes to publicly-traded companies, and obviously there's a lot of proprietary information. You all have worked with businesses, and what I'm struggling with a little bit is understanding if the thefts are material, and once they are material, they need to be reported. So is there an incentive for companies to act like ostriches, put their head in the sand and not know because they don't want to have to go public with the information, that a billion dollars' worth of their intellectual property has been stolen and it will have an impact on their earnings?

MR. BEJTLICH: You have nailed it. Our CEO Kevin Mandia has said several times that he's called many times a week by companies saying "the following has happened to me, what do I do? Do I tell someone?" And they say "what will make this breach material?"

And the experience has been if you report the breach, it becomes material, which is a terrible--it's completely counter to what we're trying to promote, I would imagine. However, I would say that if you're a publicly-traded company and you are not telling your shareholders that you've had a breach, that that is directly contrary to the SEC's guidance.

Now, of course, this could be seen as another disincentive to go public, but be that as it may, that to me is the place where you've got to apply leverage.

COMMISSIONER BARTHOLOMEW: Because you're lying. You're lying to your shareholders and to your potential shareholders if you are not admitting that this sort of thing has happened.

MR. BEJTLICH: Well, I don't know if I would go so far as saying lying because many of these companies just don't know how to think about this. They don't know what it means to have had their IP stolen, and you can't necessarily say because the IP was stolen, it's going to end up in a competing product. I think that would be kind of naive.

But many of the companies just don't know how to value what they have, but still I would err on the side of it has to go into the disclosure.

COMMISSIONER BARTHOLOMEW: And you have said, one of you had said, that 94 percent of the companies learn about the compromise from a third party, much of which is government-related third parties.

Do they have any mechanism to report to the SEC, for example? Is there any incentive or reason for them to have to say to somebody else in the U.S. government that this has happened? I'm trying to figure out ways to break open this privacy which is preventing things from moving forward?

MR. BEJTLICH: The only structures that I'm aware of are ones that, for

example, by contracts or certain members of the defense industrial base by virtue of being part of a framework that they've signed, they have to report, they have to provide certain evidence and that sort of thing. Outside of that, you don't see quite as much.

MR. VILLENEUVE: One of the things I notice is that a lot of times companies, people expect the attackers to steal design documents or things that would be kind of locked away or secured, but a lot of times, the attackers are more interested in the simple things that people don't realize are such a valuable source of information like e-mail.

So one of the things that often happens when the attackers break into a system is they force the compromised computers to download tools that allow them to start accessing people's e-mail on the mail servers in the network. And a lot of people look at that and think it's not a big deal; it's my e-mail. But contained in there is actually a lot of really valuable information that is as valuable as those design documents you have locked away.

COMMISSIONER BARTHOLOMEW: Mr. Healey.

MR. HEALEY: I like the idea of regulating for transparency. I think the SEC guidance has done a great job for transparency without government overreaching. There are other ways that that can be done. California ten years ago passed a law saying that if the information of any Californian is disclosed or compromised, then the company has to tell them.

I was working at a bank at the time, and that drove us globally to say, all right, if a large database, for example, gets taken, we're going to tell everybody because we don't want to just tell the Californians. That's bad press, and what if we get it wrong? What if we get someone that was a Californian and we didn't know?

Great way of getting the word out there in a different manner than just whether it's material or not. It's much more black and white.

COMMISSIONER BARTHOLOMEW: It's interesting, too, because if you think about doing that sort of thing, it also provides an incentive for companies to harden their systems because then they don't have to report if there is some sort of theft that has taken place. So thank you.

HEARING CO-CHAIR WORTZEL: We have a few minutes left, and three Commissioners that wanted to either finish up or ask a second question. So if we can really do it in about two minutes each, we will get through that, and the first is Commissioner Fiedler.

HEARING CO-CHAIR FIEDLER: I just wanted to follow up on your elucidation of a problem of counterintelligence. In old forms of counterintelligence, the problem that was allowed to continue was small, was narrow, not as great as we're talking about here. So it seems to me that there's a requirement to rethink that. This gets to the public, and it's a very controversial

role of the National Security Agency, the top practitioners on our side and their role in public-private partnerships.

What's your view?

MR. BEJTLICH: Just from the privacy perspective, and this is coming from an old Air Force intel guy, I fear that the public would be too suspicious of the NSA having the lead documenting role for this. I think it would have to be run through DHS, maybe with NSA as support provider or expertise provider, but if the NSA were known as being a lead role, I mean EPIC is suing the government to find out what's going on between Google and NSA, and that was to me, that's probably the biggest cyber breach in terms of publicity that we've had in the last couple of years.

MR. HEALEY: And NSA has been fairly clear that they want to collect signals intelligence, and I'm a SIGINT, I'm also an Air Force intel officer, Signals Intelligence, and it's time to stop collecting. It's time to give up, and it's time to want to win.

HEARING CO-CHAIR FIEDLER: Thank you.

HEARING CO-CHAIR WORTZEL: Thank you.

Commissioner Cleveland, you want to ask your European question?

COMMISSIONER CLEVELAND: Can we just go back to what's your sense of how cooperative the Europeans would be? Back to the question that I asked earlier about the Europeans and what their reactions would be?

MR. BEJTLICH: Sure. I had firsthand experience dealing with the Brits. They are very much interested in this. I've also seen public pronouncements by the Germans and the French directly calling out the Chinese that this has to stop. So just looking at those three countries, I think there would be some consensus.

MR. VILLENEUVE: Yes. I'm Canadian, and we face a lot of the same, the same problems, and in terms of the scope of the activity we see, although a lot of people are focused on activities that happen in the U.S., we definitely see the same campaigns having targets in the European countries as well.

MR. HEALEY: So I think there is room for the countries to come together and come up with a common approach, and I think the more that the U.S. government can come up with non-technical solutions, you know, the more we talk about monitoring, the more it's going to sound like deep-packet inspection, and the more it's going to put the Europeans off into a data privacy fight that we just don't need to have. There's lots of other ways to address this.

MR. BEJTLICH: And just a quick note on that as well. The Japanese are terrified. They are doing a lot of work this year as a result of things that were announced publicly last year. So there would be a great place to work as well.

COMMISSIONER CLEVELAND: Can you all come up with, for the record, a couple of, I mean sort of what the best approach is in terms of coming up with a

coordinated or universal, not universal, but a coordinated response?

Thanks.

MR. BEJTLICH: Yes.

MR. HEALEY: Certainly.

HEARING CO-CHAIR WORTZEL: Commissioner Reinsch, or Vice Chairman Reinsch, you want to finish up here?

VICE CHAIRMAN REINSCH: Well, I'll just go back to what I asked. Is there any solution? Anything to be done about the employee problem?

MR. HEALEY: I think, based on what I have seen, and many more people on the Commission have more experience in China than I do, it seems like there was something about Chinese culture. It was not yet seen as wrong to pirate Microsoft or jump from one country to another and take the secrets.

So in that sense, we're just a symptom of that problem, that if they're not worried about stealing from each other, why would they be worried about stealing from us?

So I think the more things that we can do to help address that problem, and it might even be possible that China is going to develop that itself, that it says if we're going to really be a power and really, really want intellectual property for our own companies, we have to support this.

MR. BEJTLICH: I actually welcome any time I see a physical component because we have a long established history of knowing how to deal with people. They have addresses, they have histories, there's background checks, there's all sorts of things we can do that we just cannot do for someone remote, 5,000 miles away, at a keyboard.

I used to joke with my counterpart in the physical security part of General Electric that my goal was to make my cyber problem his physical problem.

[Laughter.]

MR. BEJTLICH: Because once it was a question of spies and that sort of thing, we knew how to deal with that a lot easier.

HEARING CO-CHAIR WORTZEL: Well, it also strikes me that when you're dealing with a country that doesn't have a tradition of rule of law, either noncompete, you can't go to work for a competitor, or nondisclosure agreements are pretty much unenforceable.

Gentlemen, this has been a very rich discussion. We really appreciate your time. Some of the other Commissioners wonder if they submitted some written questions to you, would you be willing to contribute some other things for the record?

MR. BEJTLICH: Yes.

MR. HEALEY: Yes.

HEARING CO-CHAIR WORTZEL: Well, thank you very much. We're going to break now--for what--50 minutes; is it?

HEARING CO-CHAIR FIEDLER: Yes.

HEARING CO-CHAIR WORTZEL: All right.

HEARING CO-CHAIR FIEDLER: 12:50.

HEARING CO-CHAIR WORTZEL: 12:50 we'll reconvene. Thank you again.

[Whereupon, at 12:00 noon, the hearing recessed, to reconvene at 12:52 p.m., this same day.]

PANEL II – FISSILE MATERIAL PRODUCTION AND NUCLEAR COOPERATION

HEARING CO-CHAIR FIEDLER: In the interest of being on time, welcome back. This is our second panel of the day, and we'll address China's fissile material production, its international nuclear activities and related areas.

Joining us today are two seasoned experts in the field: Henry Sokolski and Dr. Philip Karber.

Mr. Sokolski is Executive Director of the Nonproliferation Policy Education Center. Previously he served in a variety of posts in the Pentagon and intelligence community. He's also been appointed to two congressional commissions. So he's going to be quite familiar with the seven-minute rule.

MR. SOKOLSKI: You have my condolences.

[Laughter.]

HEARING CO-CHAIR FIEDLER: Dr. Karber is adjunct professor at Georgetown University and has several decades of experience in defense and security policy, particularly nuclear issues.

You'll each have seven minutes to make your presentations, and the reason we do that is so that the Commissioners can ask you many more questions. Thank you.

Dr. Karber.

OPENING STATEMENT OF DR. PHILLIP A. KARBER
ADJUNCT PROFESSOR, GEORGETOWN UNIVERSITY

DR. KARBER: The focus of my comments, it actually probably in some ways makes more sense if Henry went first, but we're going to interrelate so it doesn't really matter.

Henry is going to address in his paper the issue of China's fissile material and fissile production. I was going to address that partially in my presentation, but towards the end. My major focus is on China's "Underground Great Wall," which went public last summer and still is relatively unknown in terms of a lot of the details. I mean there's been some controversy, but many of the operational and even strategic implications of it have not been addressed so I thought I'd use this today to summarize that, and then, in fact, that comes back to the issue of fissile material.

On the 11th of December 2009, China announced that they had been working since 1985, for 27 years, 29 years, on an "Underground Great Wall." That's their name for it. And by their definition, a facility to hide nuclear weapons and missiles.

The aspects associated with the Underground Great Wall do not include civil defense. They do not include the 40 some airbases that have tunnel and underground complexes, and they don't include the dozen or so naval complexes. It's just the strategic rocket forces, their missiles, and the country's nuclear weapons assets.

What's interesting about that, if you'll turn to the slides, hopefully, that each of you have, I'll just refer to a few of them in passing, is that this slide shows the growth in the number of those length of the tunnels. These are actually PLA numbers, having listed about 2,500 kilometers' worth of tunnels in 1995, and 5,000 kilometers cumulative in the last year-and-a-half.

The sheer size and magnitude of that, to give you an idea, would be the largest--if it's true--would be the largest construction project in recorded human history. There's nothing else man has done that would equal the size and scale of that activity.

The issue was reported in China. It also was reported in Asia in December, but basically did not get mentioned in the Western press until last summer. So for about 22 months, it essentially went unnoticed in the Western press.

There are three major aspects that I would say ought to call your attention. First, I'll call it the tactical operational issue. The majority of China's missile force is tactical and operational; that is, they cover theater targets and tactical targets. That's the DF-21, the DF-15, DF-11 and DH-10 cruise missile. Those missiles are a substantial amount of these--account for much of these

tunnels.

While the numbers of launchers of those missiles are less than 400, they equate to over 1,500 missiles, and what the Chinese appear to have done is incorporate the tunnel complex into a warfighting strategy at the tactical and operational level. That is the missile units are kept--most of their assets are kept in the tunnels on alert. People are brought in, units are ready. On a signal, they then literally surge out of the tunnels along with lots of decoys, go to firing positions, can go into launch, and then either reload out in the open or go back into the tunnel complex and even a different tunnel complex to fire those systems.

The second, and understanding that operational theater issue, particularly in light of the fact that we and the Russians have gotten rid of most of our equivalent systems under the INF Treaty, and our forces and our allies are extremely vulnerable in Asia, of course, is worth giving some serious thought to.

Second major aspect I would encourage you to take a look at is the growth in the size of the tunnels, not just that they are growing in the length, but the sheer volume of them. I've included about a dozen pages in here, just because these photographs essentially haven't been shown. Almost all of them are captured from Chinese TV. All the construction crews working on them are Second Artillery. That is they are rocket force people. These aren't civilian contractors.

And you'll notice the sheer size of them. Some of them are larger width and height than this room, and you can actually see into infinity down a corridor perhaps a half a kilometer of that kind of facility.

That is that it can hold not just one missile, but actually three trains' worth of missiles. The reason that's important is there seems to be an association with their new strategic rocket forces and these large tunnels. That would include the mobile DF-31 ICBM, what appears to be a larger mobile system, sometimes described as, again, road mobile, called the DF-41, larger because it could probably contain missiles as well, and then we've also seen photographs of what they call the intercontinental ballistic missile train, and that train has been seen going in and out of tunnels.

So what you might have here then is a substantial part of their strategic forces that could actually target the United States being in these tunnels.

The United States, depending on who and how one counts, various estimates go the Chinese have a nuclear force of 100 to 400 warheads. Generally, that's focused on operational systems. It does not count reserve warheads, which we can go into and describe in more detail.

I don't know how many nuclear weapons the Chinese have. I know that they've been producing them for over 40 years. The early production rates in

the late '60s and early '70s and early '80s of about seven a year would at that rate give them today a total, and if it continued, a force structure of over 3,000 warheads.

I can and will talk to you about the force structure. Their force structure could certainly handle that many warheads. But let's assume they don't. Let's assume that basically because of either the limitations on fissile material or policy, they haven't built those warheads.

What's significant about the tunnel complex is it is a matter of their choice. They could start producing. I have a slide in here showing the growth of China's fissile material, planned purchases of reactors. If you look at the sheer growth of their planned reactors, whatever your assumptions are today about whether they have a fissile limitation or not, there's a serious issue that they are unlikely to be fissilely limited in the future.

And the significance of that is that if that is combined with a force structure which can have nuclear missiles then put on top of conventional launchers, which they can, you're in a position where they could actually change the strategic balance, certainly the tactical and theater balance, very quickly and would go virtually undetected because of the tunnel complex.

So the combination of the tunnel complex and a robust force structure and a future potential for fissile material has a very significant breakout potential, and I think it is worth the Commission giving considerable attention to it.

I'm not trying to demonize the Chinese. They have every right to do it. They're not limited by treaty. On the other hand, they themselves have been extremely ambiguous about much of these aspects, and they ought to be confronted and held accountable.

Thank you.

HEARING CO-CHAIR FIEDLER: Thank you.
Mr. Sokolski.

OPENING STATEMENT OF HENRY SOKOLSKI
EXECUTIVE DIRECTOR, NONPROLIFERATION POLICY EDUCATION CENTER

MR. SOKOLSKI: First of all, I want to thank you for inviting me to testify. I don't know where the next one is going to be. I barely got here, but I got here just in time.

I guess if there are only two things to take away from what I'm going to say today it's that, first, I don't think we know how many nuclear weapons China has or might get relatively quickly; and two, if we're serious about our own defense planning, our security alliances, and nuclear arms reductions, we need to find out.

Unfortunately, China keeps all of this information secret. Here's I think a base case of what we might know. Enriched uranium, which is one of the key ingredients to make bombs, China operates several relatively new Russian-designed centrifuge plants that enrich, and they have an indigenous centrifuge plant, and the estimates looking at the buildings in the pictures is that probably two million SWUs, or separate work units.

The most highly regarded unclassified estimates made by the International Panel on Fissile Materials is that China has 16 tons of weapons-grade uranium plus or minus four tons. That gives you some idea of the uncertainties. That's enough to make between roughly 1,000 crude first-generation design weapons and maybe as many as 3,000 if they used advanced designs.

If you know anything about what they know about our weapons designs, I think you should assume they are very advanced.

As for plutonium, it's unclear to what extent, if any, China has dismantled the existing plants, but we know they've been shut down. We can check with thermal signatures.

If one assumes even the most conservative estimates made by, again, this International Panel, China could build an arsenal of as many as 450 crude--that's Nagasaki style because we're talking plutonium--devices, and roughly twice as many if they have advanced designs.

I might add we don't know how much plutonium these plants have produced when they were shut down. So there's a lot of uncertainty here.

As for electrical power plutonium-related activities, China currently has a pilot reprocessing plant and wants to buy an enormous plant from AREVA--the French--that could produce a thousand crude bombs' worth of plutonium annually.

It's decided to place this civilian facility right next to its major nuclear military production facilities, which one Chinese lady told me they did because it would be convenient, and that can be taken a number of different ways.

From this discussion, it's easy to see how difficult it is to pinpoint how many nuclear warheads China has and how many it could produce quickly. To cope with these uncertainties, most experts, who cluster their estimates around 200 deployed nuclear weapons depend heavily on how many nuclear missiles there are--this is the reason I think Phil's here--may not know that number.

They also assume a single large thermonuclear warhead in almost every case for each long-range missile that's observed and a few gravity bombs and spares.

Now a lot is presumed here, and almost all the assumptions are rebuttable. They include there are no missile reloads, that the cruise missiles are only conventionally armed, that there are no tactical weapons on the battlefield, that everything is a large thermonuclear warhead that consumes a lot of fissile material in each case.

Now, I think, as I said, all of these assumptions and others are rebuttable, but even if one makes them, there's a problem. Recently, one of the nation's leading experts on Chinese nuclear forces knocked down concerns that China might have 3,000 deployed nuclear warheads. He explained in some detail why theoretically the Chinese could have no more than 1,660 nuclear weapons, i.e., roughly the number of warheads the U.S. currently has deployed.

His analysis, of course, was intended to reassure, but it's difficult to see how such a wide range of uncertainty could do anything but rattle.

Why? Well, we've got four reasons why. First, such estimates bear directly on how threatening China's military might be. It's fair to note, and I've seen people on the right and left both say this, that what matters is how willing a country is to use what they have, not the number of weapons they have.

That may be, but I think the willingness to risk or engage in nuclear conflict or threaten to do so may turn on calculations of how many targets it might be able to destroy in a nuclear first strike and how many of its nuclear systems might survive after an adversary has struck.

In these matters, to paraphrase Stalin, quantity may have a quality all of its own.

Second, and related to how many weapons China may have and how willing it is to use them, is how we might prepare our defenses and the Russians or other countries. I don't think, you know, either Washington or Moscow would like to consider a future in which the Chinese had so many nuclear weapons it would feel confident about using its conventional weapons, which are quite advanced now.

They would try to deal with this in a variety of ways, everything from

missile defenses to maintaining certain strike capabilities. So that number may matter in that regard.

Also, Chinese nuclear numbers ultimately relate to how much arms control we'll engage in. I don't think either the United States or Moscow would go very low, and we're now talking about going to a thousand or as low as 300, if they thought it would end up giving China an advantage in numbers.

Finally, there's the question of how these numbers might impact the activities of neighboring states like Japan, South Korea, and India. In the first instance, Japan and South Korea are in the throes of trying to decide whether to recycle plutonium that could be used not only in civilian reactors but bombs, and recycle it in a big way.

India, of course, is trying to gauge how much it needs to build up to deal with Pakistan and China.

In consideration of all this, I've got four recommendations. First, I think you need to demand that our government do more in classified and unclassified forums to clarify what it thinks China has in the way of a deployed number of nuclear weapons and reserve nuclear warheads.

How much nuclear weapons materials and nuclear weapons usable material production capacity does it have?

We can also work with our allies, and to the extent possible, I would recommend we work with China. I don't know that there is much you can do with them, but I would go through the motions at least.

Gaming, which is I guess really Phil's suggestion--I'm taking his idea here--with senior officials about these questions and possible military crises scenarios and how all the numbers might alter or not alter these scenarios and possible arms control negotiations with Russia and other states is something that would be useful to do. I don't think it's been done, certainly not the latter, with arms control.

Also, I would explore nuclear missile talks, initially with Russia and China and then other countries, and in these talks, the most threatening missiles are the ground-based nuclear capable missiles. We have them in silos. Russia has them on ground mobile systems, and China has many of them, as you just heard, in tunnels.

I think these are the drivers of uncertainties with regard to China, and therefore it would be a useful thing to discuss.

Finally, I would get China, South Korea, and Japan to follow America's example, and foreswear making more highly-enriched uranium or recycling plutonium either for civil or military purposes.

Not knowing what they're doing, much less what they've done, is part of the general package, and we need to bear down on this diplomatically.

Thank you. That concludes my presentation. I would ask that the

copy of my testimony that I have, which corrected two or three grammatical errors, be the one that's used in the record.

PREPARED STATEMENT OF HENRY SOKOLSKI
EXECUTIVE DIRECTOR, NONPROLIFERATION POLICY EDUCATION CENTER

China's Nuclear Weapons and Fissile Materials Holdings:

Uncertainties and Concerns

By

Henry Sokolski

Executive Director

The Nonproliferation Policy Education Center

www.npolicy.org

Testimony before the U.S. Economic and Security Review Commission

"Developments in China's Cyber and Nuclear Capabilities"

March 26, 2012

George Mason University, Manassas, VA

Mr. Chairman, members of the commission, I want to thank you for allowing me to testify before you today on the question of what China's nuclear weapons materials holdings and production might be and what the security implications might be of the U.S. and other states not having clear answers to these questions.

Some of What We Know

As the most definitive current, public assessments of Chinese fissile materials assets and

production capabilities notes in the 2010 *Global Fissile Material Report*, there is little official information about China's nuclear arsenal. One can speculate but, as this analysis explains,

Without knowledge of the operating history and power of China's plutonium-production reactors and the capacities of its uranium enrichment plants, any estimates of China's fissile material stocks will necessarily have great uncertainties.[1] China, unfortunately, keeps nearly all information about its stocks of fissile materials and nuclear weapons secret. Unlike the other four other permanent members of the United Nations Security Council, China has made no declaration of how much fissile material it has in excess of its military requirements or announced whether or not it has ceased production of weapons plutonium or uranium.

Regarding current production of enriched uranium, China is known to operate several relatively new Russian-designed uranium centrifuge enrichment plants and an indigenous centrifuge plant that are believed together to be capable of producing roughly 2 million separate work units (SWUs) per year.[2] The International Panel on Fissile Materials offers a conservative estimate that China has 16 tons of weapons grade uranium (plus or minus 4 tons) – enough to make between roughly 1,000 (crude first-generation design) and 3,000 (advanced design) nominal 20-kiloton explosive devices.[3]

As for plutonium, it is unclear to what extent, if any, China has dismantled its existing military plutonium production plants but it is believed to have shut them down. Precisely when they were shut down and precisely how much plutonium they produced is not known. The most definitive, public estimates of how much plutonium China has produced presume that the plants in question, which have not been visited, are "like" ones that China built underground for reserve production and has recently put on public display.[4]

As a result, estimates of how much separated plutonium China has on hand are hardly hard and fast. If one assumes even the most conservative estimates made in the International Fissile Material Panel report of 2011 (i.e., 1.8 tons), though, China could build an arsenal of as many as 450 crude plutonium devices and roughly twice as many advanced designed plutonium warheads.[5]

---

[1] See International Panel on Fissile Materials, *Global Fissile Material Report 2010: Balancing the Books, Production and Stocks*, pp. 97-98., available at http://fissilematerials.org/library/gfmr10.pdf.

[2] See International Panel on Fissile Materials, *Global Fissile Material Report 2011: Nuclear Weapon and Fissile Material Stockpiles and Production*, January 2012, available at http://fissilematerials.org/library/gfmr11.pdf. For reference, it takes roughly 200 separative work units (swus) to produce 1 kilogram of weapons grade highly enriched uranium (HEU) and roughly 20 kilograms of HEU to make a crude nuclear weapon. A crude nuclear weapon is defined as a first generation device like that used in the Second World War. The Hiroshima bomb used 29 kilograms of HEU and the Nagasaki bomb used 6 kilograms of plutonium. Today, a first generation bomb is assumed to require a bit less HEU (20 kilograms) and plutonium (4 kilograms). An advanced weapons design would reduce the amounts of fissile required to produce a given yield by between a factor of two and a factor of three. On these points, see Thomas B. Cochran, "The Problem of Nuclear Energy Proliferation," in Patrick L. Clawson, editor, *Energy and National Security in the 21st Century*, (Washington DC: National Defense University Press, 1995), pp. 96-99.

[3] The approximate fissile material requirements for crude and advanced design highly enriched uranium nominal 20 kiloton nuclear weapons -- 16 and 5 kilograms -- is taken from Cochran, "The Problem of Nuclear Energy Proliferation," p. 98 cited above in note 2.

[4] See *Global Fissile Material Report 2010*, pp. 20-21.

[5] *Global Fissile Material Report 2011*, p. 18. As detailed in note 122, this estimate is for a plutonium bomb requiring between 4-5 kilograms of separated plutonium, i.e., a crude weapons worth. An advanced weapon

As for electrical power plutonium activities, China currently has a pilot reprocessing plant that can separate plutonium from spent fuel and is planning on having AREVA build it a much larger plant capable of separating nearly 1,000 crude bombs' worth of plutonium annually. China wants to site this reprocessing plant adjacent to a major nuclear military production facility at Jiayuguan.

Some of What We Don't

Just from this brief discussion, it is easy to see how difficult pinpointing precisely how many nuclear warheads China has, how many it might build with the non-militarized nuclear materials it has on hand, and how many it might be able to build in the future. To cope with these difficulties, the most popular estimates, which cluster close to 200 deployed nuclear weapons, depend heavily on how many nuclear missiles China has deployed. A single, large, thermonuclear warhead is assumed for each observed long-range nuclear missile. A few gravity bombs for bomber delivery are added along with a handful of spares.

Much is presumed here. Among the assumptions are that there are no missile reloads for any of growing number of Chinese mobile missile launchers, that most of the growing number of long-range Chinese cruise missiles are solely conventional, that there are no Chinese tactical nuclear weapons, and that the Chinese have fielded mostly or entirely large, thermonuclear warheads that use large amounts of fissile material rather than smaller, less fissile consumptive designs.

All of these assumptions may or may not be warranted. At a minimum, we risk confusing ourselves by emphasizing only the most optimistic assumptions. Recently, one of the nation's leading experts on Chinese nuclear forces knocked down concerns that China might have 3,000 deployed warheads. He explained, in some detail, why theoretically the Chinese could have no more than 1,660 nuclear weapons, i.e., roughly the number of warheads the U.S. currently has deployed. His analysis, of course, was intended to reassure. Yet, it is difficult to see how such a wide range of uncertainly could do anything but rattle.[6]

What to Worry

As the U.S. and Russia try to reduce or contain their nuclear weapons deployments, most other nuclear weapons states (France, UK, Israel, Pakistan, India, North Korea) would require at least one to three decades of continuous, flat-out military nuclear production to catch up even to U.S. and Russian reduced nuclear weapons numbers. It is quite clear, moreover, that none of the listed states have yet set out to meet or beat the U.S. or Russia as a national goal.

China, however, is a different matter. It clearly sees the U.S. as a key military competitor in the Western Pacific and in North East Asia. It also has had border disputes with India and historically has been at odds militarily with both it and Russia. China has actively been modernizing its nuclear-capable missiles to target key U.S. and Indian military air and sea-bases with advanced conventional munitions

---

design plutonium weapon might use half as much or less. See note 2 below.

[6] See Hans Kristensen, "No, China Does Not Have 3,000 Nuclear Weapons," *FAS Strategic Security Blog*, December 3, 2011, available at *http://www.fas.org/blog/ssp/2011/12/chinanukes.php*.

and is developing similar missiles to threaten U.S. carrier task forces on the open seas. In support of such operations, China is also modernizing its military space assets, which include military communications, command, surveillance, and imagery satellites and an emerging anti-satellite capability.[7]

Would China want to ramp up its nuclear weapons capabilities? We don't know.

In its official military white papers since 2006 and in other forums, Chinese officials insist that Beijing would never be the first state to use nuclear weapons and would never threaten to use them against any nonnuclear weapons state. China also supports a doctrine that calls for a nuclear retaliatory response that is no more than what is "minimally" required and to use nuclear weapons only for its defense.[8]

Most Western Chinese security experts have interpreted these statements to mean Beijing is only interested in holding a handful of opponents' cities at risk, which, in turn, has encouraged interpreting uncertainties regarding Chinese nuclear warhead deployments toward the low end.

What China's actual nuclear use policies might be, though, is open to debate. As one analyst recently quipped, with America's first use of nuclear weapons against Japan in 1945, it is literally impossible for any country other than the U.S. to be first in using these weapons. More important, Chinese officials have emphasized that Taiwan is not an independent state and that under certain circumstances it may be necessary to use nuclear weapons against this island "province." Finally, there are the not so veiled nuclear threats that senior Chinese generals have made against the United States if it should use conventional weapons against China in response to a Chinese attack against Taiwan (including the observation that the U.S. would not being willing to risk Los Angeles to save Taipei).[9]

It is fair to note that how willing China is to use the nuclear weapons it has may be more important than how many nuclear weapons it may have. Yet, a country's willingness to risk or engage in nuclear conflict may well turn on calculations of how many targets it might be able to destroy in a nuclear first strike and how many of its nuclear systems might survive after an adversary has attempted to strike back. In these matters, quantity, to paraphrase Stalin, may have a quality all of its own.

Does China only have 200 or so nuclear weapons? Perhaps. But if nuclear-capable missile deployments is the current driver of how many nuclear weapons China has deployed, perhaps not. The

---

[7] See Ian Easton, "The Asia-Pacific's Emerging Missile Defense and Military Space Competition," January 3, 2001, available from *www.npolicy.org/article_file/The_Asia-Pacifics_Emerging_Missile_Defense_and_Military_Space_Competition_280111_1143.pdf*.

[8] On China's no first-use policies see China's 2008 White Paper, "China's National Defense in 2008" available from *www.fas.org/programs/ssp/nukes/2008DefenseWhitePaper_Jan2009.pdf;* also see analysis of this paper by Hans M. Kristensen, "China Defense White Paper Describes Nuclear Escalation," *FAS Strategic Security Blog*, January 23, 2009, available from *www.fas.org/blog/ssp/2009/01/chinapaper.php;* and M. Taylor Fravel and Evan S. Medeiros, "China's Sear for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security*, Fall 2010, available from *www.belfercenter.ksg.harvard.edu/files/Chinas_Search_for_Assured_Retaliation.pdf*.

[9] See Jonathan Watts, "Chinese General Warns of Nuclear Risk to US," *The Guardian*, July 15, 2005, available from *www.guardian.co.uk/world/2005/jul/16/china.jonathanwatts*; and Mark Schneider, "The Nuclear Doctrine and Forces of the People's Republic of China," Comparative *Strategy*, Spring 2009, available from *www.tandfonline.com/doi/abs/10.1080/01495930903025276#preview*. Also see an earlier version dated 2007, available from *www.nipp.org/Publication/Downloads/Publication%20Archive%20PDF/China%20nuclear%20final%20pub.pdf*.

Chinese, after all, claim that they have built 3,000 miles of tunnels to hide China's missile forces and related warheads and that it continues to build such tunnels.[10] If we can't see all of the nuclear-capable missiles China might have, there's a chance it may have more than we currently assume. If, in turn, the number of such missiles is a major driver of Chinese nuclear warhead deployments, the later number could be much higher than most assume.

How much larger? We don't know. It is in our interest, however, to find out.

Indeed, the first issue such uncertainty raises is how sound current U.S. and Russian nuclear modernization and missile defense plans are. It hardly would be in Washington's or Moscow's interest to let Beijing believe it could risk using Chinese conventional forces (including China's growing fleet of conventional missiles) to threaten Taiwanese, Japanese, American, Indian, or Russian targets because China's nuclear forces could out deter Russian or American nuclear forces.

Another question a large Chinese nuclear strategic force would raise is how it might impact Washington's and Moscow's current strategic arms negotiations. How eager would the U.S. and Russia be to make much deeper nuclear weapons cuts if they thought China might, as a result, end up possessing more deployed weapons than either Washington or Moscow? Appendix I (below) suggests why this might be a worry. If so, wouldn't we have to factor China into our arms control calculations?

Finally, there is the question of how China's nuclear arsenal and potential ramp up capabilities might impact the nuclear activities of states besides the U.S. and Russia.

Interested Parties

Japan would certainly be one neighbor to watch. It already has nearly 2,500 weapons worth of separated plutonium on its soil that it was supposed to use to fuel its light water reactors and fast reactors. Now, however, Japan has decided not to build more nuclear power reactors domestically. It also is reviewing the merits of continuing its fast reactor efforts, a program that is technically premised on Japan expanding its current domestic fleet of light water reactors.

A related and immediate operational question is whether or not Japan will bring a $20 billion civilian nuclear spent fuel reprocessing plant capable of producing 1,000 bombs worth of plutonium a year at Rokkasho on-line as planned in late 2012. This plant and Japan's plutonium recycling program can be tied to internal Japanese considerations in the late 1970s and early 1980s for developing a plutonium nuclear weapons option. Although this plant is not necessary for the management of Japan's spent fuel, the forward costs of operating it could run as high as $100 billion over its lifetime.[11]

In light of the questionable technical and economic benefits of operating Rokkasho, it would be difficult for Tokyo to justify proceeding with this plant's operation *unless* it wanted to develop an option to build a nuclear weapons arsenal. What, then, would one have to make of a Japanese decision to open

---

[10] See "Yamantau," *GlobalSecuirty.org,* available from *www.globalsecurity.org/wmd/world/russia/yamantau.htm*; and "What's Going On in the Yamantau Mountain Complex?" *Viewzone,* available from *www.viewzone.com/yamantau.html*.

[11] On these points, see Von Hippel, "Plutonium, Proliferation and Radioactive-Waste Politics"; Henry Sokolski, "The Post-Fukushima Arms Race?" *Foreign Policy Online,* July 29, 2011 available from *www.foreignpolicy.com/articles/2011/07/29/the_post_fukushima_arms_race* ; and Takuya Suzuki, "Nuclear Leverage: Long an Advocate of Nuclear Energy, Nakasone Now Says Japan Should Go Solar," *The Asahi Shimbun,* July 22, 2011, available from *www.asahi.com/english/TKY201107210339.htm*.

Rokkasho if this decision came on the heels of news that China actually had many more nuclear weapons than was previously believed?

South Korea, which has attempted to get its own nuclear weapons at least once, and is asking the U.S. to back Seoul's efforts to separate "peaceful" plutonium from U.S.-origin spent fuel in Korea, is sure to be watching what Japan decides. After North Korea's sinking of the Cheonan and the bombardment of Yeonpyeong Island, South Korean parliamentarians called for a possible redeployment of U.S. tactical nuclear weapons. Washington, however, rejected this request.[12] This raises the worry that Seoul might again consider developing a nuclear weapons option of its own. South Korea already has its own nuclear-capable rockets and cruise missiles. How North Korea might react to South Korea developing a nuclear weapons option is anyone's guess.

In addition to Japan and South Korea possibly reacting negatively to news of a Chinese nuclear ramp up, there is India. It already has hedged its nuclear bets with plans to build five unsafeguarded plutonium-producing breeder reactors by 2020 and by laying the foundations of an enrichment plant that may double its production of weapons-grade uranium.[13] It too has roughly 1,000 bombs worth of separated plutonium it claims it can convert into nuclear weapons. It also has pushed development of a nuclear submarine, submarine launched ballistic missiles, missile defenses, and long-range cruise missiles. Late in 2011, it announced it was working with Russia to develop a terminally guided intercontinental ballistic missile in order to off-balance Chinese medium range ballistic missile deployments near India's borders.[14] India has never tried to compete with China weapon-for-weapon but if Chinese nuclear warhead numbers were to rise substantially, India might have no other choice but to try.

Pakistan, of course, will do its best to keep up with India. Since Islamabad is already producing as much plutonium and highly enriched uranium as it can, it would likely seek further technical assistance from China and financial help from its close ally, Saudi Arabia. Islamabad may do this to hedge against India whether China or India build their nuclear arms up or not. There is also good reason to believe that Saudi Arabia might want to cooperate on nuclear weapons related activities with Pakistan to help Saudi Arabia hedge against Iran's growing nuclear weapons capabilities.

---

[12] See Julian Borger, "South Korea Considers Return of US Tactical Nuclear Weapons," *The Guardian*, November 22, 2010 available from *www.guardian.co.uk/world/2010/nov/22/south-korea-us-tactical-weapons-nuclear*; and David Dombey and Christian Oliver, "US Rules Out Nuclear Redeployment in South Korea, Financial Times, March 1, 2011 available from *www.ft.com/cms/s/0/e8a2d456-43b0-11e0-b117-00144feabdc0.html#axzz1oCEG4jBm*.

[13] See "India to Commission Breeder Reactor in 2013," *Express Buzz*, February 20, 2012, available from *www.expressbuzz.com/nation/india-to-commission-breeder-reactor-in-2013/365268.html*; and Paul Brannan, "Further Construction Progress of Possible New Military Uranium Enrichment Facility India," *ISIS REPORTS*, October 5, 2011, available from *www.isis-online.org/isis-reports/detail/further-construction-progress-of-possible-new-military-uranium-enrichment-f/7*.

[14] See "Russia to Provide 'Seeker' Tech for Agni-V ICBM," *Pakistan Defense*, October 26, 2011, available from *www.defence.pk/forums/indian-defence/136928-russia-provide-seeker-tech-agni-v-icbm.html*; Air Marshal (retd) B.K. Pandey, "Agni-V to Be Launched By March End," *SP's Aviation.net,* available from *www.spsaviation.net/story_issue.asp?Article=900*; "Why Is This DRDO Official in Moscow?" *TRISHUL*, October 5, 2011, available from *www.trishul-trident.blogspot.com/2011/10/why-is-this-drdo-official-in-moscow.html*.

What to Do

What this discussion clearly suggests is that it would make sense for our government to take more concerted action alone, with its allies and friends, and with Russia to clarify and constrain China's offensive strategic military capabilities.

Clarify What China Has or Will Have

In the first instance, this means clarifying precisely what strategic forces China has deployed and is building. Beijing's recent revelations that it has built 3,000 miles of deep tunnels to protect and hide its dual-capable missiles and related nuclear warhead systems more than suggests the desirability of reviewing our current estimates of Chinese nuclear-capable missile and nuclear weapons holdings.

It also would be useful to know what China is planning to do to expand its existing forces. How much military fissile material does China currently have on hand? How likely is it that it has or will militarize or expand these holdings? How many missile reloads does China currently have and is planning to acquire? Have or will the Chinese develop multiple warheads for its missiles? If so, for which missile types and in what numbers? How many nuclear and advanced conventional warheads is China deploying on its missiles, bombers, submarines and artillery? What are its plans for using these forces? How might these plans relate to China's emerging space, missile defense, and anti-satellite capabilities? All of these questions and more deserve review unilaterally, in classified and unclassified annual assessments, with our allies and, to the extent possible, in cooperation with the Chinese.

Game the Future

It also would be helpful to game alternative war and military crises scenarios relating to China's possible use of these forces at a senior political level in the U.S. and allied governments. Such gaming would likely impact allied arms control and U.S. and allied military planning. With regard to the later, a key focus would have to be on how one might defend, deter, and limit the damage Chinese nuclear and nonnuclear missile systems would otherwise inflict against the U.S., its bases in the Western Pacific, America's friends and Russia. This could entail not only the further development and deployment of active missile defenses, but of better passive defenses (e.g., base hardening and improving the capacity to restore operations at bases after attacks) and possibly new offensive forces (e.g., more capable, long-range conventional strike systems) to help neutralize possible offensive Chinese operations.

Such gaming also should prompt a review of our current arms control agenda. In specific, it should encourage discussion of the merits of initiating talks with China and Russia and other states about limiting ground-based, dual-capable ballistic and cruise missiles. Unlike air and sea-based missiles, these ground-launched systems can be fired instantaneously and are easiest to command and control in protracted nuclear exchanges – ideal properties for employment in a first strike. These dual-capable missiles also can inflict strategic harm against major bases and naval operations conventionally.

Explore 'Nuclear Missile' Controls

Ronald Reagan referred to these weapons as "nuclear missiles" and looked forward to their eventual elimination. Toward this end, he concluded the Intermediate Nuclear Forces (INF) Treaty agreement, which eliminated an entire class of ground-based nuclear-capable missiles, and negotiated

the Missile Technology Control Regime (MTCR), which was designed to block the further proliferation of nuclear-capable systems (i.e., missiles capable of lifting 500 kilograms or more at least 300 kilometers). With the promotion of space-based missile defenses, he hoped to eliminate all such ground-based missiles.

What states have an incentive to eliminate these missiles? The U.S. has no intermediate ground-launched missiles. It eliminated them under the INF Treaty. Most of our shorter range missiles are either air-launched or below MTCR range-payload limits. As for our ground-based ICBMs, they are all based in fixed silos and as such are vulnerable to being knocked out in a first strike. Russia, on the other hand, has a large, road-mobile ICBM force. Yet, Moscow too is worried about growing Chinese precision missile strike capabilities that it cannot defend against.[15]

India and Pakistan have ground-launched ballistic missiles but some of their most seasoned military experts have recently called for the elimination of short-range missiles since these can only serve to escalate border disputes. As for China, it has much to gain by deploying more ground-launched missiles unless, of course, it causes India, Russia, and the U.S. to react. The U.S. has been developing hypersonic boost glide systems that could provide it with prompt global strike options. It also has hundreds of silo-based ICBMs that it could affordably convert to deliver conventional warheads precisely. None of this would be in China's interest. Talks about reducing such nuclear-capable ground launched missiles, should be explored.[16]

Encourage China and Its Neighbors to Forswear Making HEU or Plutonium

Finally, although it may not be possible to conclude a fissile material cutoff treaty, all of the other nuclear weapons state members of the United Nations Security Council should press China to follow their lead in unilaterally forswearing making fissile material usable for weapons (i.e., recycling plutonium and making highly enriched uranium or HEU). In this regard, it would be helpful to call for a limited moratorium on commercial reprocessing with China and as many other states as possible. The U.S. Blue Ribbon Panel on nuclear energy recently determined that it would not be in America's interest to pursue commercial reprocessing in the near or mid-term. Japan, meanwhile, is reviewing its own commercial reprocessing and fast reactor program given its decision to move away from nuclear power. South Korea wants to recycle plutonium but is having difficulty persuading the U.S. to grant it permission to do so with the many tons of U.S.-origin spent fuel South Korea has.[17]

---

[15] See Jacob Kipp, "Asian Drivers of Russian Nuclear Force Posture" in this volume; and Dr. Mark B. Schneider, "The Nuclear Forces and Doctrine of the Russian Federation and the People's Republic of China," testimony given October 12, 2011 before the House Armed Services Subcommittee on Strategic Forces, available from *www.worldaffairscouncils.org/2011/images/insert/Majority%20Statement%20and%20Testimony.pdf*.

[16] For a fuller discussion, see the "Missiles for Peace" chapter by Henry Sokolski in this volume. Also listen to audio of a panel discussion "Missiles for Peace" held at the Carnegie Endowment for International Peace held in Washington, DC, September 13, 2010, available from *www.d2tjk9wifu2pr3.cloudfront.net/2010-09-13-Sokolski.mp3*.

[17] See "U.S Unlikely to Allow S. Korea to Reprocess Nuclear Fuel: Diplomat," Yonhap News Agency, March 3, 2012, available from *www.english.yonhapnews.co.kr/northkorea/2012/03/08/23/0401000000AEN20120308007100315F.HTML* ; and Frank Von Hippel, "Plutonium, Proliferation and Radioactive-Waste Politics in East Asia," analysis published on The Nonproliferation Policy Education Center website January 3, 2011, available from *www.npolicy.org/article.php?aid=44&rid=2*; and Takuya Suzuki, "Nuclear Leverage: Long an Advocate of

China is committed to having AREVA build it a commercial reprocessing plant that is nearly identical to the one Japan is now reconsidering opening late next year at Rokkasho. As already noted, these "peaceful," commercial reprocessing plants can produce at least 1,000 bombs worth of nuclear weapons-usable plutonium annually. Still, they are not technically necessary for the operation of nuclear power and are uneconomical compared to using fresh fuel and not recycling it. Promoting a limited plutonium recycling moratorium, in short, would be useful and could garner some support for more general fissile material production restraints.

Nuclear Energy, Nakasone Now Says Japan Should Go Solar," *Asahi.com*, July 7, 2011, available from *www.asahi.com/english/TKY201107210339.html*.

APPENDIX I

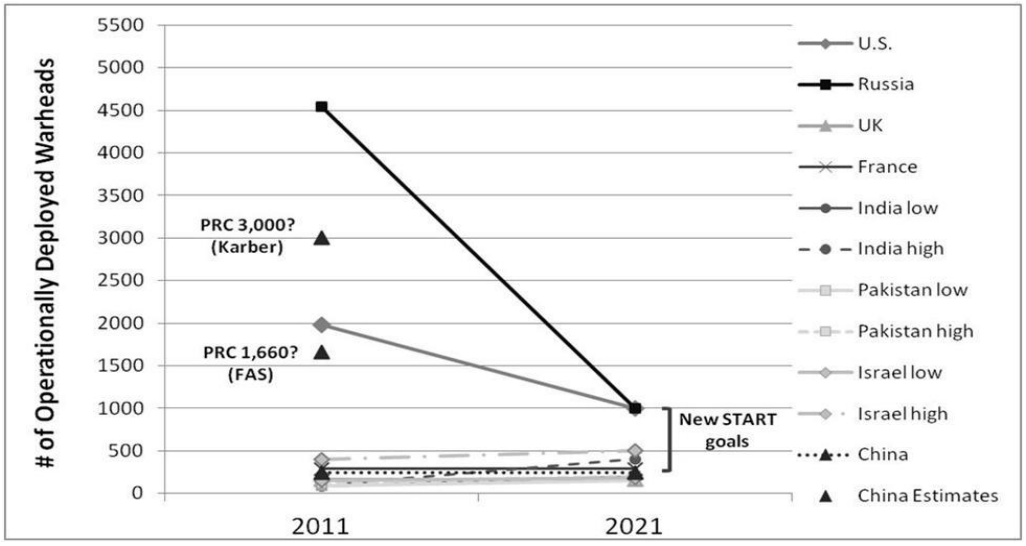

Figure 1: The Next Decade, Nuclear Uncertainties and Competitions

The numbers used to generate this chart came from U.S. Department of State, "New START Treaty Aggregate Numbers" Fact Sheet; Robert S. Norris and Hans M. Kristensen, "US Tactical Nuclear Weapons in Europe, 2011," *The Bulletin of Atomic Scientists* Vol. 67, No. 1, January/February 2011, pp. 64-73, available from www.bos.sagepub.com/content/67/1/64.full; Zia Mian, A.H. Mayyar, R. Rajaraman, and M.V. Ramana, "Fissile Materials in South Asia and the Implications of the U.S>-India Nuclear Deal," in Henry Sokolski, ed., *Pakistan's Nuclear Future: Worries Beyond War*, Carlisle, PA: Strategic Studies Institute, 2008, pp. 167-218; Shannon N. Kile, Vitaly Fedchenko, Bharath Gopalaswamy, and Hans M. Kristensen, "World Nuclear Forces," *SIPRI Yearbook 2011*, available from *www.sipri.org/yearbook/2011/07;* "Nuclear Weapons: Who has What at a glance," *Arms Control Association*, available from *www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat;* "status of World Nuclear Forces," *Federation of American Scientists*, available from *www.fas.org/programs/ssp/nukes/nuclearweapons/nukestatus.html;* Alexander Glaser and Zia Mian, "Fissile Material Stockpiles and Production, 2008," *Science and Global Security*, Vol. 16, Issue 3, 2008, pp.55-73, available from *www.tandfonline.com/doi/abs/10.1080/08929880802565131;* Warner D. Farr, "The Third Temple's Holy of Holies: Israel's Nuclear Weapons," *USAF Counterproliferation Center,* Counterproliferation Paper No. 2, September 1999, available from *www.au.af.mil/au/awc/awcgate/cpc-pubs/farr.htm;* and Kenneth S. Brower, "A Propensity for Conflict: Potential Scenarios and Outcomes of War in the Middle East," *Jane's Intelligence Review*, Special Report No. 14, February 1997, pp. 14-15; Robert S. Norris and Hans M. Kristensen, "US Nuclear Forces, 2011," *Bulletin of the Atomic Scientists* Vol. 67, No. 2, March/April 2011, pp. 66-76, available from *www.bos.sagepub.com/content/67/2/66.full;* Robert S. Norris and Hans M. Kristensen, "Russian Nuclear Forces, 2011," *Bulletin of the Atomic Scientists* Vol. 67, No. 3, May/June 2011, pp. 67-74, available from *www.bos.sagepub.com/content/67/2/66.full;* Robert S. Norris and Hans M. Kristensen, "Global Nuclear Weapons Inventories, 1945-2010," *Bulletin of the Atomic Scientists*, Vol. 66, No. 4, July 2010, pp. 77-83; William Wan, "Georgetown Students Shed Light on China's Underground Missile System for Nuclear Weapons," *The Washington Post*, November 29, 2011; Hans Kristensen, "No, China Does Not Have 3,000 Nuclear Weapons"; and Robert Burns, "US Weighing Steep Nuclear Arms Cuts," *Associated Press*, February 14, 2012, available from www.boston.com/news/nation/washington/articles/2012/02/14/ap_newsbreak_us_weighing_steep_nuclear_arms_cuts/.

PANEL II: QUESTIONS AND ANSWERS

HEARING CO-CHAIR FIEDLER: It will be entered. As long as you give it to us, so done.

MR. SOKOLSKI: It's all done. Your staff got it this morning.

HEARING CO-CHAIR FIEDLER: Let me ask Dr. Karber a quick question. You took somewhat of a beating in the press when your report came out, and if I understood you correctly, and correct me if I'm wrong, you're not saying they have 3,000, you're saying that they have the capacity in underground tunnels to handle 3,000 weapons? Isn't that correct? All right.

DR. KARBER: Could I explain that for--

HEARING CO-CHAIR FIEDLER: Please do. Let's be clear.

DR. KARBER: I happened to be on the advance team for Secretary Carlucci in Moscow when the first discussions about Nunn-Lugar were going on, and we were out at Russian Strategic Rocket Force Command facility, about 30 klicks out of Moscow, and we were having a discussion with a couple of lieutenant generals from the Soviet army about how many--initially, Nunn-Lugar, we were going to offer them railroad, special railroad train cars for moving nuclear weapons, and the permissive action link containers for warheads.

So we we're talking to the general, and the general was very dismissive and said we can build our own railroad cars, we don't need that, but the warhead containers would be interesting. You seem to be ahead of that and so forth. So we said, oh, well, how many of those would you need? And he said, well, we would need about 40,000.

And I was a little slow on the draw, and I go, why do you need two of those for each of your warheads because for 15 years, our national intelligence estimates had said that the Russians had stocked and were only at 22,000 warheads.

My colleague who was with me was a little smarter, and she said you mean you have more warheads than 22,000? And, in fact, the Russians had 42,000 warheads.

Now if you go through that personal experience, that means we missed 20,000 Russian nuclear weapons at the height of the Cold War, and we didn't just do it in one estimate. We did it repeatedly over a 15-year period.

So if one is in that, has personally experienced that, it perhaps makes one overly jaundiced about estimates based on a whole host of assumptions about what other people have when they're intentionally trying to hide stuff.

So that's sort of the background. Now my specific reference to the comment was twofold. One is we have seen Chinese references to the safe distance they would like between systems that are underground, and that

describes a thousand meters from a low air burst. So if you take the radius of that, it would be roughly a mile apart. So if you had 3,000 miles of tunnels and you wanted to put warheads in them, using that calculus, you would have room to put a thousand, 3,000 warheads in there.

There's a second issue, and that's their force structure, and this I want to be very clear about because I think people have made statements that are demonstrably wrong and can be clearly shown. If you, say, take the DF-11s and 15 tactical missiles, both we and the Russians and, I believe, the Chinese have developed warheads that essentially can go on the missile.

You can have a conventional warhead on the missile. You can have a nuclear warhead on the missile--on the same missile and the same force structure. The force structures are designed to have multiple fires. So, for example, in NATO with our tactical system, the Lance, we had for one Lance launcher, we had ten nuclear warheads.

So if you look at China's force structure right now, you could easily absorb 3,000 nuclear weapons, not only in the tactical systems, which we rate as not having any nuclear capability despite their testing or claiming they've tested an ER warhead, reloads for the DF-21s, and systems that don't get mentioned very often, naval nuclear weapons. We've seen stuff in their literature about having nuclear weapons on attack boats, which could be a torpedo, a cruise missile, or a mine.

And we've seen the recent tests and their discussions about ballistic missile defense. It's not at all clear that that ballistic missile system that they're testing is not designed to have a small nuclear weapon on it and actually be used in conjunction with the forces that are in the tunnel for protection.

So the short answer to your question is, no, I did not predict or say they have 3,000 warheads. What I am saying is it's going to be extremely hard for us to know when and how many they do have if we conclude that they have a higher stockpile of fissile material.

HEARING CO-CHAIR FIEDLER: And it's wiser that we assume more than fewer.

DR. KARBER: My first point would be, of course, would be to not assume anything and confront them and ask them, and point out to them, that we have the option of assuming the worst, but they have the option of helping us understand so we don't assume the worst.

HEARING CO-CHAIR FIEDLER: There is a point, just one quick question to both of you, there is a point where the number doesn't matter as much over a certain number, but low numbers, 400, is a meaningful thing. Maybe, I mean hypothetically, there may be no meaningful difference between 2,500 and 3,000 strategically; right?

DR. KARBER: Right.

HEARING CO-CHAIR FIEDLER: But 400--but the difference between four and 2,500 is huge.

DR. KARBER: Can I just give you two real quick examples? In the theater, we have or our allies have forces there, we have withdrawn all of our tactical and operational nuclear weapons from the Asian theater. TLMs are gone. Nuclear artillery is gone. Tactical air is gone. The only thing we have left are the B61 bombs that have to be brought into the theater, and those go on very vulnerable air bases.

Now, right now, we hold that China has no tactical nuclear systems, and yet the missiles that could carry nuclear weapons, right now, today, by DoD recognition of their numbers, not creating any more, would be in excess of 1,200. So that's 1,200 to zero.

We--the Russians got rid of our INF systems. They have 120 DF-21s, assuming no reloads and assuming that only 70 of those are nuclear. But all 120 could be nuclear. That's in the theater. Right now we assume that they have only 20 ICBMs that can hit the United States with single warheads. But if you go to the--just MIRV, the D-5, right now, with five MIRVs, that goes to a hundred. If you go to ten MIRVs per launcher, which it certainly has the throw-weight to do, and you suddenly have 200 American cities that are held hostage.

The difference between 20 and 200, I would argue, is huge psychologically in a crisis. I'm not talking about--

HEARING CO-CHAIR FIEDLER: No, I understand.

Larry.

HEARING CO-CHAIR WORTZEL: Thank you very much, both of you. This is your William Wan, "Digging Up China's Secrets" slide, Washington Post, November 30, 2011.

One of the things, these little tidbits of information on there, is Chinese references cite up to ten reloads per transporter/erector/launcher.

If you just look at the figures the federal government has given out, 400 launchers, maybe 1,500 missiles, that's four reloads. You just said that perhaps 70 DF-21s--

DR. KARBER: 70.

HEARING CO-CHAIR WORTZEL: 7-0. May be nuclear capable.

DR. KARBER: That's what the U.S. government says.

HEARING CO-CHAIR WORTZEL: Right. That means 280 to 700 nuclear warheads. I mean that's a big difference.

Now, and I recognize the gap you pointed out. My dilemma is, and it's something Henry pointed to, there's an arms control advantage in minimizing the number of warheads you have because the other side may disarm more or deploy less missile defense. But what's the strategic advantage of hiding this total number of warheads if your stated goal is minimal deterrence?

I mean you're already up to mutually assured destruction with that many warheads. So, strategically, why would the Central Military Commission of China want to hide all these numbers? Why not just go for complete deterrence as the Soviet Union?

DR. KARBER: I know--this may be a limitation on our research--but I know of no Chinese military document that says they have a minimum deterrent strategy. They have a strategy, they say they have a strategy of no first use with certain caveats.

The imposition of a minimum deterrent is a Western construct, and that has been superimposed on, in my opinion, their strategy to try and explain it. I myself believed that until I started doing research into their history. I thought at least in the early years, they had a minimum deterrent strategy, and then only recently did they go to warfighting.

We went back and looked at their exercises and the details of what they were doing even with their tactical and operational systems, the early DF-2s and DF-3s. They were doing warfighting with those in terms of the targets and the allocation of warheads. So I think, first of all, that needs to be seconded and put to rest.

Secondly, I think their concept, and I had some actual quotes from some of their major documents, Science of Second Artillery Campaigns, Science of Military Strategy, and Science of Military Campaigns, and these are their documents that they use to train their senior officers on, and what's interesting is they do not describe that. They have a term which they call "deterrence campaigns," and what a deterrence campaign is, either in a crisis period prior to a war or in the middle of a war, one suddenly reveals a larger and much more robust force structure than the opponent thinks you have.

And the concept is to get the opponent then to back down in a crisis or a conflict and not escalate, and this is actually called a "deterrent campaign." It's a formal military operation, which combines decoys and moving many additional assets and so forth. So I think built into their construct is this concept--and I'm not saying that they don't have the term "deterrence." It's interesting. If you look at the Chinese characters for deterrence, their terms are not passive like "inhibit" or "dissuade." It's extremely forceful, in your face, pressure, cower, so forth.

What's interesting about it, and then you sort of say why, why do they have such a more--what Tom Schelling would have called a compellant orientation rather than a deterrent orientation? Part of it is they were well trained. We and the Russians, every time they acted up, in the '50s, '60s and '70s, we'd march up and down the coast with a fleet, we'd put nuclear weapons on Taiwan, and we didn't mind rattling them. We taught them if we were tough, you should see what the Russians did with them, in terms of saying, yeah, nuclear weapons count and

got in their face and we'd maneuver them and deploy these things.

So the Chinese learned, hey, when you don't have much, and you get a nuclear weapon, and you're in a bargaining position with somebody who has them, suddenly revealing nuclear force can be extremely powerful and get you to back down. So I think it's built into their strategic concept.

HEARING CO-CHAIR WORTZEL: You're also suggesting, though, that three or four U.S. scholars actually constructed what we infer to be China's strategy, and you've never seen it in Chinese doctrine.

DR. KARBER: You see them referring to the American scholars.

HEARING CO-CHAIR WORTZEL: Right.

DR. KARBER: Particularly their diplomatic and arms control people, but in terms of the military, no.

HEARING CO-CHAIR WORTZEL: Thank you.

HEARING CO-CHAIR FIEDLER: Michael.

COMMISSIONER WESSEL: Thank you, gentlemen. Henry, welcome back.

Dr. Karber, I'm not a military expert. What are the refueling, not refueling, fueling implications? Can that be done underground? Many of their delivery vehicles use liquid fuel; correct? Can that be done underground? Do we have any advanced notice therefore once they take the items out of the Great Wall, out of the tunnels?

DR. KARBER: That was a real serious problem we had with the DF-2s and 3s, and the 4s and 5s. But the 2s and 3s, which were their tactical and operational theater systems, they basically would take them out and assemble the warhead externally and then fuel them because what happens, if you fuel them inside the tunnel, the fumes from that can be extremely lethal, volatile and lethal.

With the DF-11 and 15 that replaced the 2s and the 3s, and the DF-21s, those are all solid fuel missiles now. So you do not have the fueling issue with the tactical and theater issues. They're gone. There may be one training DF-3 regiment left, but all the rest are gone. So they've essentially completely converted their entire tactical theater force structure to solid fuel missiles, and that also, of course, goes for the DH-10 cruise missile.

The DF-4, which was a continental missile, was basically a missile designed to sort of cover middle Russia, and are apparently all gone now. So the only liquid fuel system left is the DF-5. They were put in silos.

It's interesting. You see numbers somewhere between four and 20 silos. The Chinese themselves say they've created a number of silos that were basically fake decoys so it's not clear exactly how many DF-5s they have. So I think the normal number people assume is about 20 that are still liquid fuel.

Several times they have changed the fuel mix in the DF-5 to give it

more throw-weight and perhaps less volatility. The silos appear to have the air-conditioning aspects of it so you can actually fuel it. It's not clear whether they have to pop the top of the silo or not to fuel it safely.

What's interesting is that system now appears to be receiving the MIRV missiles. So if you'd have asked me, I would have expected them to sort of retire it, but because it has the throw-weight like of our old Titan, and you can put, in theory, ten very decent-sized MIRV missiles on it, and they appear to be keeping it. It's interesting that they're retaining them.

Now that ties in then with the recent test of a ballistic missile defense because we've seen discussions of them actually using low-yield nuclear weapons to intercept over the ICBM silos and detonate, essentially create fratricide among our incoming RVs. They would ride it out and then do the defense, very much similar to the original U.S. safeguard system, which had the long-range intercept, ex-atmospheric interception and the short range low-yield Sprint.

And it's interesting that they seem to be looking at that, but the answer to your question is, yes, they appear to have the missiles fueled in the system and also maintain their warheads. In the various photographs that went into the artist sketch that Dr. Wortzel--we see lots of that going on.

So the tunnel complexes, they'll have these mini-laterals where they store missiles. The TEL, the Transporter/Erector/Launcher, will come into one of these big bays. It's our term calling it a gallery. You'll see rail lines consistently in those, and then they bring in on little tracks the replacement missile. There's usually a Gantry crane over top, and it picks them up, and then with the missile mount, the warhead would already be mounted and it's already fueled, and you're good to go.

You would also perhaps load up several reload vehicles that would go out with them so you could have several reloads out in the field, and that may be why we're only assuming four reloads per launcher, one on the launcher and two or three on the reload vehicle, but, in theory, the tunnel complex, it not only could, but is designed to, have substantially more, and we see them in their exercises when they describe it. And not talking about just conventional--nuclear. They talk about being out, having fired the missiles, taking incoming nuclear hits to the unit; the unit goes into a new tunnel complex and does what they call reconstitute, reorganize, reconstitute, reload the systems and go out on another firing campaign.

COMMISSIONER WESSEL: Okay. Henry, any thoughts on recent proliferation issues since that's one of the statutory mandated issues for this Commission? What should we be looking at or cognizant of these days?

MR. SOKOLSKI: Pakistan.

COMMISSIONER WESSEL: Okay.

MR. SOKOLSKI: Quite a state.

COMMISSIONER WESSEL: Okay.

MR. SOKOLSKI: Watch it. It will set the last of the precedents you need to have wild, wild West policy. We have already one policy for North Korea. I guess we have a different one for India. We had a kind of implicit policy toward Syria. And we're about to get another new one for Pakistan where we will blink. They will supply reactors. They will claim they were grandfathered when they weren't, and we will let it happen.

In addition, most of the production capability that you see, particularly with plutonium, gets lots of Chinese help, to say nothing of the missile technology.

So that one is pretty in your face. It's not--you don't even have to speak--

COMMISSIONER WESSEL: You don't have to look for networks or do all the--

MR. SOKOLSKI: --or do anything to get at that information. Just the Washington Post will do. You should be able to crack the code on that one.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR FIEDLER: Dennis? Or Dan. Excuse me.

COMMISSIONER BLUMENTHAL: Thank you.

Very good testimony and I've heard it all before, but it's good every time.

[Laughter.]

COMMISSIONER BLUMENTHAL: It's like seeing the Godfather. So I mean I'm convinced from both of you there's enough fissile material there to do whatever you want without much control. There's every reason there's enough warheads and there are enough missiles and so on, and then you look at what the U.S. can do conventionally. You know, if I'm in China, I'm thinking this might be a good idea to go up in nuclear weapons.

But I'm not in China. So what are they thinking? And if it is more compellant, at what point were they going to roll out this compellant nuclear force or did they put out enough so that you could find it?

In other words, if you're going to compel somebody, you have to actually demonstrate that you have a force to compel them. I find the story compelling I mean because if you all of a sudden shock people and say that you might have 1,500 or even more warheads or you're rushing to parity, then, yeah, you're going to get the whole region's attention. No question. Particularly when we're going down.

So why haven't they been more forthcoming about compelling? That's sort of Larry's question. Why hide it? Or maybe they didn't. Maybe they let you see, maybe they let you see stuff, and Phil Karber was the one who picked it up.

MR. SOKOLSKI: Maybe they don't have it.

DR. KARBER: I think, first of all, they've had throughout the period, you have to remember that China came to the modern era from essentially being grossly inferior.

COMMISSIONER BLUMENTHAL: Right.

DR. KARBER: We and the Russians came to it from having superiority at various times. We certainly, and even the Russians vis-a-vis China. And so we're aware of all the limitations of superiority, the stuff is only usable sometimes, and it's frequently not that useful of a device for compellance.

If you've been a victim of compellance, however, you have a different perception of it. So there's a danger, I think, of us symmetrically looking at and imposing our view on it. I think given that in their view, Deng Xiaoping had a statement that went something like "hide your light in the darkness, but build your capability." I'm not doing justice to it. Larry, I'm sure, will remember.

Hu Jintao has repeated that as recently as two years ago. I think their general philosophy was, build up your capability until you're ready, and then don't, and don't get in their face. Now, it's interesting, 2009 was the 60th anniversary of the PRC, and in Chinese cosmology, the 60 years, 12 years is a cycle, and you have five cycles, which completed what symbolically would be the equivalent of a century for us. It's really an important meaningful term, a 60-year period.

So it was interesting, in the spring, in 2009, in the spring, they had the huge naval review like they'd never had. You'd think it was the Queen of England. In the summer they had the largest exercise they'd ever had in the history of the PLA including anti-terrorism exercise with 3,000 tanks, which was sort of cool.

[Laughter.]

DR. KARBER: You had the huge parade, which they made much of, and you had the first air show in October. Well, Second Artillery hadn't had its thing. It didn't have its day in the sun throughout that whole year, and so my impression is that the announcement on December 11, 2009, was their coming out as well, which was, okay, we're doing these, we now have 3,000 miles of these tunnels.

It's interesting that we paid almost no attention to it. I mean virtually the story was ignored both officially and in the press, and yet in their press, they would go, oh, the Americans--I can show you titles, "Americans Are Shaking Over the Revelation that We Have 3,000 Miles of Tunnels." So, in their mind, they had this impact on us even though we know it wasn't real.

Now, what's interesting also is that Hu Jintao in his speech on the anniversary said the last previous 60 years was coming out from our weakness. Now, we have in the next 60 years a new era in which China is strong.

So I don't think it's accidental that they came out with this announcement. In fact, I think the announcement is very fragrant in terms of its

implications.

I think operationally we're likely to see stuff at their convenience when they decide they want to do it. My guess is it's between now and 2020. In other words, I'm not predicting next week there's going to be a sudden event.

Two things I would watch for: one is a crisis, in which in the crisis they unveil a lot of stuff that we had not seen. You saw perhaps a precursor of that during the nasty stuff going on in the summer of 2010 in the South China Sea when they were making their usual chest-thumping, and then they went and fired 71 live missile fires in the South China Sea. It was an extremely intense missile campaign that, again, we hardly noticed but made huge waves--excuse the pun--in Southeast Asia.

The other is with the strategic forces. When they're ready, when you see the 41 out there and the 5s are MIRVed, and we're starting to talk in our annual posture statements about a China with two or 300 warheads aimed at the United States, I think you're going to see then them acting as if that's true, and that's going to be a very different approach than the current one.

COMMISSIONER BLUMENTHAL: Thank you.

HEARING CO-CHAIR FIEDLER: Commissioner Shea.

CHAIRMAN SHEA: Thank you, both, for being here.

Earlier this morning, we heard from General Cartwright, the former Vice Chairman of the Joint Chiefs, and he said that one of the things that concerns him is this apparent split between the civilian leadership and the military which manifests itself periodically, for example, at the ASAT test.

Do we know enough about who controls China's nuclear force and fissile material? I would assume that the individual who gives the authorization for the use of the nuclear weapon would be the Chairman of the Central Military Commission who would be the General Secretary of the Communist Party. But do we know enough about how they make decisions and what's going on there?

DR. KARBER: One of the reasons I subtitled my testimony, "American Strategic Entropy," using the word "entropy," is because to me the entropy is having an idea what it is you don't know.

And so my view is, no, we do not know, we do not know what we ought to know or need to know about it. So now I think there are people who will give you very strong, good evidence and track and are much more expert than I am on that specifically.

Three quick comments. One is it appears accurate, and I know nothing that would be inconsistent with the concept, that the Central Committee, Central Military Committee and its chair are at the top of the chain. On the other hand--and in terms of the structure systems, I think Mark Stokes is America's living expert on the allocation of the special warhead detachments and I think there is a misleading deal that when people say they have them centralized, it's not like it's

in one facility, but they do appear to be centralized out in the various base locations, and then the base locations have warhead distribution units.

So it's inconceivable that a number of systems that might be considered nuclear or certainly nuclear capable may not have their warheads with them in peacetime. That might be allocated to them. Why that's important--this is the third issue--is--and this is what is so unclear, in my opinion--is where does release authority and firing authority overlap?

So we know, for example, the Russians, when the Russians put the missiles into Cuba, the Central Committee gave, and the General Staff gave, release authority to the Russian general in charge in Cuba, and with that authority, he had the right to fire those FROGs that we didn't know were there.

So one wonders where that overlap occurs and when it occurs. In other words, how far down that chain it goes. Generally, what we've done has been very, very tight, and so--with our own forces-- we assume, well, you've got to have a presidential release all the way down to the fire unit. It's not clear where that is with China or where it would reside in a crisis or, even worse, in a conflict where these missiles are being fired.

They have made an interesting statement that needs to be taken into account because I think it's serious, and that this commitment to have a no first use does not apply if their territory is being attacked. That was made by the Commander of the Strategic Rocket Force.

Now what's interesting is if they're claiming that the South China Sea is sovereign territory, that itself raises an interesting issue because he didn't say attacked nuclearlyor attacked conventionally. In fact, he specifically referenced that they would not tolerate a conventional air attack like we did against Yugoslavia or Belgrade on China without responding with nuclear weapons.

So where in a conflict is that release given and then left to theater commanders, and I use the word "theater" because one thing that is really interesting that again you ought to track very carefully over the next few years is the Chinese have been building theater commands.

In the old days with the Russians, we would have called those TBDs, theaters of operation. And since 2000, they've been implementing these, and it's interesting, they say the whole theater system will be complete in the year 2020 so that will be a year tolook for this.

CHAIRMAN SHEA: Thank you.

Mr. Sokolski.

MR. SOKOLSKI: In the remaining 25 seconds.

HEARING CO-CHAIR FIEDLER: No, you got time.

MR. SOKOLSKI: Mr. Stokes did a paper for us recently on the Cultural Revolution and what happened to the nuclear arms and how they were fought over. That experience made him conclude that there is a reason in history and

culture to keep the numbers of these weapons down. It doesn't go with the flow of what we're telling you. It's useful to read. It may be right.

I want to emphasize we don't know. That means we shouldn't assume what's going to be. We need to find out.

HEARING CO-CHAIR FIEDLER: I'm with you.

Commissioner Cleveland.

COMMISSIONER CLEVELAND: Should our lack of knowledge have an effect on our discussions with the Russians about weapons reductions?

MR. SOKOLSKI: I think so on a couple of scores. First of all, I sat and listened to a very senior administration official talk about our future, the future of arms control and strategic forces.

The presentation went on for 90 minutes. It was a terrific presentation for 1990. It did not make a whole lot of sense now or ten years forward. Why? I don't think the Russians are the main event. They got a lot of things, but are they really going to fight a big war with us or our allies? I don't see it.

When I look at China, they seem to have a bone to pick with a lot of their neighbors. They have a bone to pick with us. So she did not mention--this person--China once in 90 minutes. I pointed this out. I said you should get one of those cue cards, put the word "China" in there and start talking about it.

I think it's because we have an easier time talking with the Russians, if not getting to an agreement, than we do the Chinese. The Chinese are much tougher to deal with. They don't like to talk about anything. You give them something for free. They won't take it. They're suspicious.

So what you do is you retreat from that which you can't immediately get sort of measurable progress on. I think it's a big mistake. I'll tell you why.

It isn't just the United States that ought to be curious about this. The Russians are. The more you read Russian military literature, and we've got some essays from people who do, the more you discover they're worried about China. There are very few things about which we can cooperate with Russia and be on the same frequency. This might very well be it. That we're not focusing on this is a mystery to me, absolute mystery.

By the way, you know from my days working on that commission with you, I'm no big fan of the Russians. But here maybe it would be useful to focus. We don't. I don't think we've brought the topic up.

COMMISSIONER CLEVELAND: That's interesting. Dr. Karber, do you have anything to add?

DR. KARBER: I certainly agree with everything Henry said. I would just add that I think that we have not given the intellectual capital to the issue of tripolarity. We really have not thought it through, and I don't think a lot of the lessons we learned from bipolarity necessarily apply. If you look back historically,

multipolarity is reasonably stable and bipolarity is reasonably stable.

Multipolarity is where you have lots of plays and they balance against each other. Tripolarity is extremely unstable because a combination of any two players basically offers the ability to take the other player out, and I think that's extremely dangerous. I just don't think we've thought through a lot of the implications, and so if we haven't thought them through in terms of strategic context, then one ought to do that, and then from that flow arms control.

I spent some years negotiating with the Chinese as an aviation executive. My experience is that they will tell you they don't like to negotiate, but if you sit down and say we have a problem, and here is what the likely--you're not threatening, but here's the likely consequences of where we go if we don't get an agreement and you can illustrate that to them, frequently they come around.

So, for example, if we and the Russians said we can't stay in the INF Treaty, either you're going to get in or we're going to get out--

COMMISSIONER CLEVELAND: Right.

DR. KARBER: --and we don't think that it's going to be all that attractive to you if we get out, I think that has, that kind of conversation, quiet, not threatening, thoughtful, treating them as a peer, has potential. I wouldn't bandy it as a national objective. I wouldn't even want to do it--you want to do it very, very, very quietly.

MR. SOKOLSKI: I think it's very hard to do anything very quietly anymore. So heads up. Particularly when you talk about arms control, I would generally make the same point. I don't know that I would go down that particular path to threaten to break out of the INF. I don't think we are that built up to play that game, number one.

But we do have something both the Russians and the Chinese care about, and that is turning long range missiles that have nuclear warheads into conventional missiles.

They care a lot about that. To be honest, I think they overestimate what we can do, kind of like the Russians and SDI. Good. One of the points that I make--I think I actually have a footnote--is, you know, give them the chance to reduce the ground-based missiles, which they have a lot, or then if we can't, then we have to use our ground-based missiles, which we have plenty of them in the Midwest, in a different way, which they will not like.

So there are lots of different ways you can paint a future that they might not like that they can avoid. We should at least try. We're not even playing this game, as best I can tell. By the way, what I suggest is not very expensive either.

HEARING CO-CHAIR FIEDLER: Commissioner Slane.

COMMISSIONER SLANE: Thank you for taking the time to testify.

Can you talk a little bit about the status of the anti-ship ballistic

missile?

MR. SOKOLSKI: It's sort of Mark Stokes' little baby, but I'll defer to you on that one.

DR. KARBER: It's the DF-21, the latest model, which typically is called the "D." It's an interesting scientific challenge because with a ballistic missile, the nice things about it is you get speed, they go a long distance in a short amount of time.

The problem is you're going against a moving target so there's a limit, a finite limit, to the accuracy that you can have because the issue is getting updates to where that ship will be as you're coming in the last two or three minutes.

When you're a ballistic missile and your velocity is coming in extremely fast, you actually create on the nose cone of the missile a heat plasma, and that heat plasma basically prevents most of your seekers from being able to see through that plasma.

So if you have a slow-moving missile coming in, like a cruise missile or a limited tactical missile, he can do last minute upgrades by tracking the target or getting feedback from it and controlling the missile.

So what's interesting about that missile is to offset that, they've gone through an extremely complex approach, and that is to basically take the missile and fire it in a ballistic trajectory, and then as it comes through the atmospheric and becomes atmospheric, then have the veins on it actually make it aerodynamic, and so it slows down and goes at a much lower speed and actually at a slant angle, and then that slant angle, that plasma has now slowed down so you can actually see through the plasma, and that allows you then to home in on the target and actually home in on the moving target.

That is an enormously complex scientific challenge to get that and pull that whole thing off because you not only need a missile that has those kinds of accuracies, you'd like to be able to have it updated before he actually goes into this dive because once he's in that dive, he's locked in on a very narrow trajectory so you need space assets, you need communication assets, you need something tracking that carrier initially to get him in the general basket, and then just the sheer process of getting him into that maneuver is very complex.

They have been working at it hard and seem to be making progress on it. Between now and 2020, I think it is a reasonable assumption that they will have some degree of effectiveness against particularly large ships.

What's interesting is, well, that has sort of sucked all the oxygen of our interest out of the atmosphere right now. We're all focusing on the DF-21. They have developed also a number of other anti-ship missiles: the DH-10, which has a range of about 1,000 kilometers cruise missile, very fast, very effective; the H-6 bomber carrying a cruise missile; the submarines launching cruise missiles.

And there's also the potential of high-speed cavitating torpedoes. So the issue to me, the threat, is not just that the DF-21 is one type of missile, which has got a lot of attention because it's, in fact, frankly, unique, and we have, of course, nothing to counter it, nothing that equivalent, and we couldn't without breaking the INF Treaty.

But what's interesting is in the combined arms context, when you see all of these systems coming in, that's going to be a very frightening experience for any significant capital shift within a thousand kilometers of the Chinese mainland. And that is going to push us offshore. It's also going to hold our airbases hostage, and our allies are going to see that, and then they're going to start reacting very uncomfortably.

MR. SOKOLSKI: Yeah. I think this point about the bases also needs to be amplified. If it's fixed, it's targeted now if there's range, and they've gone and learned the best they can from us about submunitions. So the numbers of missile necessary to take out soft targets and even somewhat hard targets is not that many.

So some of it is not elegant, and that in combination with whatever it is they may develop could add up to denial of sea.

I can tell you one thing. The Navy is apoplectic about this. You go up to Newport, Rhode Island, they talk about this a lot and have been for the last three or four years. They're worried.

COMMISSIONER SLANE: Do you see this evolving into an arms race?

MR. SOKOLSKI: Well, an arms race, as I learned it in graduate school, is something mechanical. Do I see it as a rivalry? Yeah. It already is. It's just one rival is working a little harder than the other in their local area, that's all. But it's already something our Navy is very concerned about.

We're already hardening various assets on forward bases in the Pacific. We're trying to figure out how to operate out there. So I mean in a sense that rivalry has already been engaged. I don't see how it couldn't.

But a race makes it sound like tit for tat, up the ante, out of control, da-da-da. I'm not so sure about that. I mean if you took a look at our Navy budget, I don't know how many ships they're building, maybe not as many fielded as they used to. So it's not quite that kind of race; it's something else.

HEARING CO-CHAIR FIEDLER: Commissioner Wortzel.

HEARING CO-CHAIR WORTZEL: I wanted--well, two things. First of all, wouldn't it be a better United States' approach to assume China has four to ten times as many warheads, plan accordingly for our own forces, and then challenge China to disabuse us of that concept so that we're not ready to face 3,000 warheads or 2,000.

And, then, second, if the CSS-2 or DF-3 is out of the operational Chinese inventory, what's in Saudi Arabia? And will they be replaced or are those

dual-capable nuclear and conventional missiles?

MR. SOKOLSKI: Any missile is dual capable depending on how indiscriminate you'd like to be. I mean what was--the CSS-2s after all are hardly great conventional precision missiles.

HEARING CO-CHAIR WORTZEL: No.

MR. SOKOLSKI: That's what they have there. So that's point one.

With regard to the Larry Wortzel op-ed that we'll see in The Washington Times, I would recommend Samuel Johnson's admonition, "strike it out." Here's why. I think the United States, for better or worse, gained a reputation for crying wolf. We don't need any more of that. I don't think you have to do that to raise what are absolutely legitimate questions that need answers.

China has made a career out of using ambiguity and silence as some kind of defense and saying, well, this allows us to do things less provocatively. Well, it does, but we're allowing them to do this by not saying, this uncertainty now is a problem. I think we need to be at least willing to say that. I don't think you'll be called to the carpet for pointing out something that's true until someone else tells us it's not true.

We need to put the burden of proof on the Chinese. I think that's enough.

HEARING CO-CHAIR FIEDLER: Second part of your question.

HEARING CO-CHAIR WORTZEL: Well, I don't know if Phil has anything.

DR. KARBER: I guess I would, I think Henry's political advice is right. That is one doesn't want to know how difficult it is. Having been subject to fairly withering fire--

[Laughter.]

DR. KARBER: --for opining that they might have something, I understand how not only the amount of the incoming coming in, but the tendency of it then to sort of create equivalence, or people sort of then dismissing your argument. So I think his point is well-taken.

But I don't like to leave it there. I think it would be worthwhile asking. And part of the problem frankly is that the U.S. intelligence community is as committed to certain sets of numbers today as they were back in the Soviet Union. The reason I like to throw that out is because they weren't perfect, but that doesn't mean they're wrong now. Okay.

So rather than get into a huge internecine debate over A teams and B teams, in which I think if they had the evidence, people would call it like they see it. I don't think they're hiding or it's a conspiracy; I think they're calling what they can see. And then the issue is all the ambiguity.

So I think an internal approach, an approach that would be prudent, would be to say set some markers and say, okay, what are things that we would

expect to see if that force posture is increasing? And it's not just the, oh, we picked up an NSA intercept that such a unit has the warhead because those can change in a relatively short matter of time.

It's the longer-leader items of what can deliver nuclear weapons, what's coming, what kind of training is going on, and watching that. And I think by identifying a number of key indicators that would allow one to track and say, okay, you get to this one, when two of these three have tripped, we better start seriously thinking about what our options are. That would be the approach.

And the last thing I--

MR. SOKOLSKI: By the way, I would not disagree that you need to do the, not just gaming, but the intelligence nit--if you will--picking by getting these intelligence requirements dialed in through the game example might be the best way to do it, but, yeah, I mean, sure, that too.

DR. KARBER: The one area just where I'm disagreeing slightly with Henry, I like the arms race metaphor in the sense that we used it in the period of the Cold War, and there was the old conundrum how do you win an arms race without going to war, and the answer was get the other side to quit, and that's what happened successfully in the last Cold War.

What I am afraid of is going on is there is, in fact, an arms race going on in the Pacific and Asia right now, and the Chinese already know the answer to it, and that is to get us to quit, and so at some point we're going to be confronted with too much expense and too large of an issue, and all of a sudden it's going to be convenient to sort of fall back or abandon those allies, and that I think is the game plan.

HEARING CO-CHAIR FIEDLER: Commissioner Cleveland. Second round.

COMMISSIONER CLEVELAND: If we haven't yet engaged with a dialogue with the Russians about a strategy, are you aware of any effort to engage with them on sharing information about what the Chinese might or might not have?

MR. SOKOLSKI: Well, I think we have engaged them a little bit on the INF question. I just think we're seized with that treaty rather than the bigger question of missiles writ large.

As for what kind of intelligence we share with the Russians and what they share with us with regard to China, I haven't a clue, but my guess is you got to give them a cause to do that, and I'm not sure we give them that. So it may be that the two things are related. Don't know.

COMMISSIONER CLEVELAND: When you say we've given them that cause, I'm sorry, I'm not following you.

MR. SOKOLSKI: I said we have not yet given them a reason to share intelligence about the Chinese.

COMMISSIONER CLEVELAND: Because we haven't sought it as opposed

to the Chinese giving them the reason to initiate?

MR. SOKOLSKI: The Russian military, as best I can tell, is seized with the advanced conventional munitions and missile capabilities of China. It is one of the reasons they argue they need nuclear weapons in such large numbers in the theater. So they get that one, but I don't know that they see advantage in any kind of condominium with the United States in pressuring or seeking more clarity or less activity on the part of the Chinese. I'm not sure about that. I'm pretty sure judging from what I've heard it's not been engaged.

COMMISSIONER CLEVELAND: You're taking it a step further than I was. I was simply thinking in terms of an exchange of information, not involving the Chinese, just the--

MR. SOKOLSKI: Well, even involving the Russians, you'd have to have a reason to do an exchange. You don't just rock up and say how about the Chinese; we've got some cards; would you like to--I think you want to have some public diplomacy dimension where that exchange makes sense.

COMMISSIONER CLEVELAND: Henry, you mentioned that the Chinese are arguing that the provision of a plant is grandfathered in the Pakistan relationship. Can you elaborate on that, and do you view the transfers that the Chinese are engaged in with Pakistan as consistent with our NSG and NPT commitments?

MR. SOKOLSKI: Well, working backwards, no and no.

COMMISSIONER CLEVELAND: Okay.

MR. SOKOLSKI: We have listened to various arguments about this grandfathering all before. The first two plants were grandfathered, you see. Now, the next two are. I don't know. I kind of feel like we're being nuclear chumps here. I think it's because that body has become so unmanageable. We've let too many members in that we don't think we can win this fight, that we've decided not to fight it. Not hard enough.

But I think that then means that we need to figure out how to tighten up the nuclear rules some other way. And we haven't done that either. So this is not looking good.

HEARING CO-CHAIR FIEDLER: Let me let Commissioner Shea have the last word this afternoon.

CHAIRMAN SHEA: This is for Mr. Sokolski. This is a little off topic, but I see that you wrote a book called Getting Ready for a Nuclear-Ready Iran.

MR. SOKOLSKI: I did.

CHAIRMAN SHEA: Could you share with us, give us a little bit of a primer on Chinese assistance or lack of assistance with respect to the Iranian nuclear program and their missile technology capabilities?

MR. SOKOLSKI: Well, the missiles have to do primarily with anti-ship missiles. I'd have to go back and get the designations, and it's been awhile ago.

The nuclear assistance had to do something that we put into plain sight and then winked. Hexafluoride plant. First, we said stop it. They wouldn't. Then we said, well, we want to sell you nuclear reactors. We can't unless you do something. So they said, all right, we'll leave, but we have to leave them with the plans, and, of course, some people hung around.

Well, we're stunned to discover that they finished that plant. That plant is critical to the nuclear enrichment effort in Iran. So that's a problem.

Then we have one other thing that's out in the open, and by the way, I'm only telling you things newspaper readers would know. Luckily, I can't remember anything that's classified on this so it's okay.

The second thing is there's been a lot of transshipment activity, you know, emanating out of North Korea to places like Syria, and we're not entirely convinced that the Iranians didn't have something to do with the Syrian effort as well. It's still probably locked up tight. Maybe there was no connection.

Some people argue there was, but those transshipments occurred with the assistance of the Chinese, and I would think if that was the case, other transshipments that might go from North Korea to Iran might well have gotten a wink and a nod. Geography. You just see what a straight line looks like. It's best to just fly over or land, and so I think there's that. And certainly I mentioned Pakistan. That one is hard to hide.

CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR FIEDLER: Yes, Dr. Karber.

DR. KARBER: If we have just one minute, I'd like to respond to--

HEARING CO-CHAIR FIEDLER: Okay.

DR. KARBER: --Commissioner Cleveland's question to Henry. One thing I think we need to look at is the other side of that tripolar equation, the Russian-Chinese thing. It's obvious that they have been selling the Chinese a lot of equipment, and it's in every single category of weaponry, and I won't go through, but it's huge, and the Russians have made some money on it, usually not as much as they had hoped because the Chinese end up stealing the design, and the Russians say never again, and they go sell something. It goes on.

[Laughter.]

DR. KARBER: They deserve each other.

HEARING CO-CHAIR FIEDLER: Sounds like the Americans.

DR. KARBER: There are a couple of things that we haven't highlighted, both good or weird, and I think ought to get higher in the consciousness as we talk about China in the context of tripolarity. One is when the Chinese actually went on a national alert in the summer of 1999, and virtually the Americans have ignored this, and this is demonstrable in their literature, and of course I believe they also went on a nuclear alert.

What was interesting is they then went to the Russians, and in either

December of '99 or January of 2000, Putin came out and actually made a public announcement committing Russian SLBMs in the Pacific to China's defense. As an obscure comment, we kind of go wow, right. But it's interesting. It's not, it generally goes unrecognized.

Now let's look at the other side. Alexei Arbatov was a long-time Russian arms negotiator, a member of their parliament. His father ran the USA Institute. He did a recent article which he was raising Russian concerns about Chinese warheads. He himself used the 3,000 number. I think he was probably bouncing off me.

[Laughter.]

DR. KARBER: What's interesting, what's interesting is we have a whole series of Russian General Staff articles that talked about China having 2,000 nuclear weapons in 1995. So the Russian concern with a large Chinese stockpile and their belief in it I think is something that would give us an area to talk about.

Lastly, particularly for those who say, oh, China doesn't believe in arms control, the largest arms control agreement since the Cold War and probably since the end of World War II is between Russia and China, and it's virtually unknown. They did a mutual forces separation agreement between the two of them and Kazakhstan that involved more forces, by my count, than all of CFE.

COMMISSIONER CLEVELAND: Wow.

DR. KARBER: Huge. And both sides, and they have annual inspections, they have annual meetings. It's a very formal treaty, and it was secret, as you basically--my students had to search for months to try and finally get a copy of it. But it's worth looking at.

And so it has verification in it, and it has--so it's not a one-sided, one-time deal. So I think looking at this, we need to start looking at the tripolar relationship, and there's a number of sides to that, that other side that I think would behoove looking at.

COMMISSIONER CLEVELAND: Who signed the agreement between Russia and China?

DR. KARBER: I'm sorry. Who signed? Who signed?

COMMISSIONER CLEVELAND: The agreement, yeah.

DR. KARBER: It was Kazakhstan, Russia and China. I don't know who signed for the authorities.

COMMISSIONER CLEVELAND: Civilian or military? I was just curious.

DR. KARBER: I'll get you a copy. Neither of the two big powers produced it. The way we got a copy was Kazakhstan.

COMMISSIONER CLEVELAND: Kazakhstan. Interesting. Thank you.

HEARING CO-CHAIR FIEDLER: Gentlemen, thank you very much.

COMMISSIONER CLEVELAND: Thank your students, Dr. Karber.

HEARING CO-CHAIR FIEDLER: We're going to take a short break before

the next panel. Five minutes.

[Whereupon, a short recess was taken.]

PANEL III: NUCLEAR FORCES AND STRATEGY

HEARING CO-CHAIR WORTZEL: We're going to start our final panel. The last panel today will examine China's nuclear forces and strategies. We just looked at fissile material and warheads.

Dr. Mark Schneider, the first panelist, is a Senior Analyst at the National Institute of Public Policy. Throughout a long career in the executive branch, he specialized in missile defense policy, nuclear weapons, deterrence, strategic forces, arms control, and arms control verification and compliance issues.

The second panelist is Dr. Phillip Saunders. He's the Director of the Center for Study of Chinese Military Affairs at the National Defense University, recently putting out a brand new publication on the Chinese Navy, and it was excellent, and previously he directed the East Asian Nonproliferation Program at the Monterey Institute of International Studies. Earlier he served as an officer in the Air Force.

Dr. Schneider, there's a little clock there, but we try and limit it to seven minutes of testimony so that we can get a lot of questions out.

Thank you very much.

OPENING STATEMENT OF DR. MARK SCHNEIDER
SENIOR ANALYST, NATIONAL INSTITUTE OF PUBLIC POLICY

DR. SCHNEIDER: Mr. Chairman, distinguished members of the Commission, I thank you for inviting me to speak before you today. This is a very important topic.

I started out my statement by quoting the section from one of the editions of the Pentagon Report on Chinese Military Power, about how much concealment and deception these guys practice, and it's a lot. And any time you talk about China, you have to keep that in mind. It's a closed society, very secretive, and it's very difficult to get information about them.

Having said that, I think we have a reasonably accurate assessment of what Chinese nuclear strategy is about, and at least some indication of what they're doing in the nuclear area.

Now, the first thing I was asked to talk about was the size of the stockpile. I agree with Phil Karber on this one: nobody knows. We can only estimate it. The estimates differ quite considerably. The official U.S. government estimate, as stated by then Principal Deputy Undersecretary of Defense James Miller, was that they had a few hundred nuclear weapons.

The Taiwanese Defense Ministry report has a substantially larger number. They estimate the Second Artillery has something on the order of 400 to, 450 to 500 weapons, and, of course, the Second Artillery is not the only nuclear armed service in China. So there's roughly a factor of two difference here between just those estimates, and, of course, you can find higher and lower estimates of what the Chinese have.

If I had to guess, it would be on the upside. I think the old World War II adage about, you know, any time you see an intelligence estimate, double it and add 30 percent is probably not a bad rule of thumb.

[Laughter.]

DR. SCHNEIDER: So we have, I think a significant Chinese force, one that is absolutely certain to grow over the next ten or 20 years. How big it's going to grow, we don't know. That will largely be determined by the extent they MIRV the new missiles that are under development, the sort of generation beyond the DF-31, DF-31A, JL-2 missiles.

A Pentagon report says the Chinese may be in the process of developing a new MIRVed mobile ICBM. That is one of the big potential threat elements. And I think this is the same missile that's being referred to in the Asian press as the DF-41.

There are also lots of reports in the Asian press about MIRVing the new Chinese SLBMs, including reports of advanced versions of the JL-2, even a JL-3, and even a type 96 submarine. So there's a lot of potential for upsize increase

in Chinese capability in that area.

As for the Chinese nuclear doctrine, I think we know a lot less about that than say we know about the Russians. I believe that most elements of what they call their nuclear doctrine in their white papers is essentially political propaganda. It's not real.

Their no first use formulation doesn't commit them to anything. I mean they literally cannot violate it, and actually Dr. Wortzel, I think, did the first good analysis on this, and when I saw his stuff and actually looked at it in detail, he was completely on the mark. There is no way you can violate that statement even if you use nuclear weapons first.

So, the other thing I felt that was sort of humorous, when they published or at least they published their so-called "nuclear doctrine," I think it was a 2006 edition of their White Paper, if you go back to the 2004 edition, it's their arms control section. So it's not real as a nuclear doctrine.

The idea of what--their "self-defense counter attack" is a multipurpose propaganda formulation that they have applied frequently when they have initiated military action, including the fairly large-scale invasion of North Vietnam in the late 1970s.

I don't have very much time so let me go through this as quickly as I can. They are certainly working on missile defense penetration aids and devices. There's not much on this in the open sources. Perhaps the best thing is the Defense Review report of a few years ago, which actually talks about some of the techniques that they are using to penetrate missile defense.

If you're really interested in this, I would ask the Missile Defense Agency to give you a classified briefing because I simply can't elaborate on that here.

In terms of sort of their hidden doctrine, the Kyodo News Agency last year said it obtained classified Chinese documents which they said they would adjust the nuclear use threshold in time of war to permit first use. I think that's quite credible. As a matter of fact, I believe it's--I don't know for sure, but I think it's one of the books that Phil Karber mentioned earlier, the Science of the Second Artillery Campaign, which is extremely revealing. It has three, actually four, instances where they would use nuclear weapons first, and three of the four are consistent with no first use.

It also says that they're directed to maintain the capability of launching a nuclear first strike any time during a conflict.

On tactical nuclear weapons, I think they've got a lot more than they're generally given credit for. The Pentagon report this year, or last year, said that the DF-21D, now that's the anti-carrier missile, has a nuclear option on it, and I have Chinese sources that say the same thing. So that's, if there's such a thing as a tactical nuclear weapon, something designed to attack a naval ship, it's

certainly it. And I think they've got a lot more than that.

They're continuing, at least the reports, that they're continuing nuclear testing. I think that's consistent with the modernization program that is going on today.

And they announced several years ago, they are in the process of building a missile defense system, and it's treated to some degree in the latest edition of the Pentagon report. Richard Fisher, some of his work, is pretty good on this in terms of what they're actually doing.

Again, to sum this up, when you look at Chinese nuclear forces and doctrine, you have to put this in the context of their overall defense strategy and military build-up. It's not isolated. And I think it's very much a part of the same troublesome pattern of double digit defense increases for 20 years, and I think we're going to see more of that in the future.

Thank you.

PREPARED STATEMENT OF DR. MARK SCHNEIDER
SENIOR ANALYST, NATIONAL INSTITUTE OF PUBLIC POLICY

March 26, 2012
Dr. Mark B. Schneider
Senior Analyst, National Institute for Public Policy
Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "Developments in China's Cyber and Nuclear Capabilities"

Mr. Chairman and Members of the Commission, thank you for inviting me to speak to you today on what I believe is a very important subject – the nuclear forces and policies of the People's Republic of China.

The annual Pentagon report on Chinese military power has observed that, "From Beijing's perspective, strategic ambiguity--including strategic denial and deception--is a mechanism to influence the policies of foreign governments and the opinions of the general public and elites in other countries."[1] Yet we tend to ignore this when looking at China. China is still a dictatorship and, as such, it is hard to obtain information on official Chinese policy and doctrine. Having said this, I believe we understand the core elements of the PRC's policy related to nuclear forces although we are far from understanding all the details.

We must remember that Chinese nuclear weapons policy is a subset of a broader national security policy. The Chinese seek to shift dramatically the balance of power in its favor, while reducing the prospect of an enhanced security response by those nations that are threatened by the Chinese military buildup which has seen double digit increases in its expenditures for all but one of the last twenty years.

Until recent (late 2010) announcements starting in December 2010 made by the Russian Federation concerning expanding its nuclear forces, China was the only member of the P-5 which was openly increasing its nuclear forces. Moreover, the Chinese nuclear buildup and modernization must be seen in the context of the more than 80% reduction in U.S. nuclear forces since the end of the Cold War and the end of significant U.S. nuclear force modernization programs in the 1990s. Had China done absolutely nothing during the past twenty years, its relative position vis-a-vis the U.S. would still have improved. Instead, it has been expanding and modernizing its nuclear forces.

I was asked to comment on the size of the Chinese nuclear arsenal. No one knows for sure other than the Chinese. We can only estimate its size. In testimony before the House Armed Services Committee in November 2011, then-Principal Deputy Under Secretary of Defense James Miller stated that the Chinese nuclear arsenal is estimated to be a few hundred weapons.[2] The Government of Taiwan's

---

[1] "FY04 REPORT TO CONGRESS ON PRC MILITARY POWER Pursuant to the FY2000 National Defense Authorization Act," Washington D.C. U.S. Department of Defense, 2004, available at: <http://www.defense.gov/pubs/ d20040528prc.pdf>.
[2] "STATEMENT OF DR. JAMES N. MILLER PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY BEFORE THE HOUSE COMMITTEE ON ARMED SERVICES NOVEMBER 2, 2011," p. 1, available at: http://armedservices. house.gov/index.cfm/files/serve?File_id=faad05df-9016-42c5-86bc-b83144c635c9

estimate of the Chinese nuclear arsenal is higher. In 2011, the Taiwan's Defense Ministry estimated that China's Second Artillery had between 450 and 500 nuclear weapons.[3] The total number of nuclear weapons would, of course, be higher because the Second Artillery does not control the nuclear weapons of the Naval or the Air Forces. (The 2008 Chinese defense White Paper says that the "Second Artillery Force will use nuclear missiles to launch a resolute counterattack against the enemy either independently or together with the nuclear forces of other services."[4]) A 1999 study by the Carnegie Endowment estimated that China had 450 nuclear weapons.[5] In November 2007, Duncan Lennox, editor of Jane's Strategic Weapons Systems stated, "It would not surprise me to learn that the actual figure [for Chinese nuclear weapons] today is around 400 to 500 and that this will increase to around 700-800 over the next decade."[6] Russian estimates of China's nuclear arsenal are generally much higher than those of the United States. I suspect that the Taiwan estimate is more accurate than our own and we are currently underestimating the likely scope of the Chinese nuclear program over the next two decades.

I was also asked to comment on the reasons why China would conceal the true size of its nuclear arsenal. Specifically the question read: "If a nation's objective is deterrence, why would that nation conceal the existence of a larger nuclear arsenal?" I believe it is necessary to keep in mind that Chinese objectives are more than simple deterrence. Warfighting plays a significant role in Chinese strategy and denial, deception, and surprise are a major part of warfighting. There are actually many reasons for concealing the size of China's nuclear arsenal: 1) China is not threatened by any attack, nuclear or otherwise, at this time and, hence, has no reason to declare fully its nuclear forces for deterrence purposes; 2) Covert nuclear forces are likely to be more survivable and have greater tactical surprise value if used; 3) Revealing the plans for the buildup of Chinese nuclear forces over the next decade would have no near-term benefit for China; 4) Hiding a large buildup of Chinese nuclear forces will likely reduce the prospects of either countervailing action on the part of the United States, and possibly even Japan, or at least reduce the probability that the U.S. will not make further unilateral reductions; and 5) Since China prefers to talk openly about arms control and reductions by others rather than engage in such negotiations involving its own forces. Chinese secrecy on the scope of its nuclear buildup reduces the prospect that China might be forced to participate in a multilateral version of the New START Treaty, as Russia has suggested.

If U.S.-China relations degenerate to the point of a major crisis where China would want to enhance its nuclear deterrent capability, China could reveal the extent of it nuclear capability at a time of its choosing. There is simply no need to do this today.

With regard to tactical nuclear weapons, concealing the existence of various weapons can have great tactical value. If the existence of a specific type of tactical nuclear capability is known, the scope of the

---

[3] "Section 2 PRC Military Capabilities and Threats," Taipei: Republic of China, Ministry of National Defense, 2011, available at: <http://2011mndreport.mnd.gov.tw/en/info04.html>.

[4] "China's National Defense in 2008." Beijing: Information Office of the State Council of the People's Republic of China, January 2009, available at: <http://www.fas.org/programs/ssp/nukes/2008DefenseWhitePaper _Jan2009.pdf>.

[5] *China's Changing Nuclear Policy, A Reaction to the South Asian Nuclear Tests*, Washington: D.C.: Carnegie Endowment for International Peace, 1999, available at: <http://www.ceip.org/pubs/china-zhang/Contents.html>.

[6] Duncan Lennox, **"**Unravelling a Chinese puzzle*," Jane's Defence Weekly***,** November 07, 2007.

threat can be mitigated by tactics, modes of deployment of military capabilities and nuclear hardening of military equipment. If the existence of these capabilities is successfully hidden, none of this is likely to happen.

I do not think the availability of fissile material will be a significant constraint on China. It is noteworthy that a declassified 1984 DIA report estimated that China had 150-160 nuclear weapons as far back as 1984 and concluded "the number of warheads is not restricted by Chinese materials production, but on what the Chinese perceive their needs to be."[7] With the massive Chinese nuclear energy program now underway, China should be able to produce as many nuclear weapons as needed.

Republican Senators on the Foreign Relations Committee in their report on the New START Treaty estimated that the Chinese nuclear force would grow to 600-1,000 weapons over the next decade. I believe we ought to take this assessment seriously. Even a thousand weapons may underestimate the scope of the Chinese nuclear force 10 or 20 years from now.

There is nothing unusual about hiding the full extent of one's nuclear capability. The Soviet Union did this. After the end of the Cold War, we found out that the Soviet nuclear arsenal was much larger than what we believed it to be during that period.

The PRC is currently increasing its strategic nuclear forces, both qualitatively and quantitatively. The Director of National Intelligence, retired General James Clapper, has said that China's nuclear forces are a "mortal threat" to the United States. Indeed, China is preparing for a war against Taiwan, which it believes may require it to fight the United States and possibly Japan. While China would certainly prefer "winning without fighting," Chinese generals have repeatedly threatened nuclear war over Taiwan. Moreover, Chinese strategic objectives go well beyond Taiwan.

According to the Pentagon, China is deploying two new intercontinental ballistic missiles (ICBMs) the DF-31 and DF-31A, developing a new submarine-launched ballistic missile (SLBM) (the JL-2), building a new type of ballistic missile submarine, at least six of which will reportedly be deployed. Taiwan confirmed the reported successful launch of JL-2 SLBMs in December 2011; this development will probably result in the relatively early deployment of these missiles.

In 2011, the Pentagon report on Chinese military power said China has between 55-65 ICBMs. Taiwan's Defense Ministry estimated that in 2011 China had over 180 "strategic missiles."[8] It did not define "strategic missile," but there still appears to be a significant difference in the numbers estimated by the Pentagon and by Taiwan.

The Chinese deploy mobile ballistic missiles which are protected by hard and deeply buried tunnel facilities. There is no doubt about this. Such facilities are very difficult to destroy. A recent study by Georgetown Professor Philip Karber has concluded that there is an absolutely massive network of

---

[7] "Nuclear Weapons Systems in China," DIA, *Defense Estimate Brief*, April 24, 1984, available at: <http://www.gwu.edu/~nsarchiv/news/19990527/01-01.htm.

[8] Ibid.

tunnels that could conceal a much larger strategic force than the Pentagon estimates to be the case.[9]

The extent of the deployment of multiple independently targetable warheads (MIRVs) on its new missiles will have an enormous impact on the size of the Chinese strategic force over the next 10-20 years. The Pentagon report has discussed Chinese development of MIRVs and China is reportedly deploying them on modernized versions of its CS-5 ICBMs.[18] According to the most recent Pentagon report on Chinese military power, the PRC may be developing a new road-mobile ICBM, "possibly" capable of carrying a multiple independently targetable warhead (MIRV). This is apparently the missile that is referred to as the DF-41 in the Asian press. *Jane*'s reports that it may carry up to 9-10 warheads. There are reports in the Asian press that China plans to MIRV its SLBMs heavily -- as many as 576 warheads on six submarines -- although no time frame is reported.[19] There are reports of a number of advanced versions of the JL-2 and the JL-3 SLBMs which may be references to the same missile or modifications of the same missile.[20]

The Pentagon report on Chinese military power has long said there were a wide variety of advanced strategic missile related research and development programs. The 2011 report reads:

> China is also currently working on a range of technologies to attempt to counter U.S. and other countries' ballistic missile defense systems, including maneuvering re-entry vehicles, MIRVs, decoys, chaff, jamming, thermal shielding, and anti-satellite (ASAT) weapons. PRC official media also cites numerous Second Artillery Corps training exercises featuring maneuver, camouflage, and launch operations under simulated combat conditions, which are intended to increase survivability. Together with the increased mobility and survivability of the new generation of missiles, these technologies and training enhancements strengthen China's nuclear force and enhance its strategic strike capabilities.[21]

In addition to strategic systems, China has a variety of medium- and intermediate-range ballistic missiles. *Aviation Week* reports that China has announced that its new 4,000-km range ballistic missile will be nuclear capable.[22] In general, China tends to deploy nuclear variants of many of its ballistic

---

[9] William Wan, "Georgetown students shed light on China's tunnel system for nuclear weapons," *The Washington Post*, November 29, 2011, available at: <http://www.washingtonpost.com/world/national-security/georgetown-students-shed-light-on-chinas-tunnel-system-for-nuclear-weapons/2011/11/16/gIQA6AmKAO_story.html>.

[18] Gennadiy Nechayev, "In Order To See Better," Moscow *Vzglyad Online*, April 9, 2010. Translated by Open Source Center Doc. ID: CEP20100412358009.

[19] Mark Schneider, "The Nuclear Doctrine and Forces of the People's Republic of China," *Comparative Strategy*, July 1, 2009, p. 259, available at: <http://www.tandfonline.com/doi/abs/10.1080/01495930903025276#preview>.:

[20] Ibid.: Toronto *Kanwa Asian Defense Review Online*, September 1, 2011. Translated by Open Source Center Doc. ID: CPP20111103715031.

[21] *ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2011*, Washington D.C.: U.S. Department of Defense 2011, p. 34, available at: <http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf>.

[22] Bill Sweetman and Richard D. Fisher, Jr., "Air Sea Battle Concept Is Focused On China," *Aviation Week*, April 7, 2011, available at: <http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2011/04/04/AW_04_04 _2011_p62-99099.xml&headline=AirSea%20Battle%20Concept%20Is% 20Focused%20On%20 China&channel=awst>.

missiles that are generally thought of as conventional. An official at Taiwan's Defense Ministry has said that the Chinese M-11 missile "can fire a variety of warheads ranging from nuclear and chemical warheads to electromagnetic pulse warheads."[10] According to the Japanese Defense Ministry, the DF-21 medium-range ballistic missile can carry a nuclear warhead.[11] The 2011 Pentagon report on the Chinese military revealed that the DF-21D, China's anti-ship ballistic missile, was part of China's nuclear deterrent force.[12] The Chinese DH-10 ground-launched cruise missile is assessed by the Air Force National Air and Intelligence Center as capable of delivering either a conventional or a nuclear warhead.[2313]

Qing Tong, writing in 2002 in a Hong Kong journal which reportedly has close ties to the PRC military, stated, "China has achieved progress by leaps and bounds in its tactical nuclear weapons, making nuclear weapons practical and facilitating their use in future high-tech, local wars."[14] In 2002, Russian officers Lieutenant Colonel O. Moiseyenkov and Captain 1st Rank A. Smolovskiy wrote that China had "tactical missile warheads and artillery rounds."[2415]

According to Richard D. Fisher, Jr. and Bill Sweetman of *Aviation Week*, "Chinese sources have referred to future DF-25/26/27 missiles: One may be the new 4,000-km missile. Future PLA [People's Liberation Army] medium- and short-range ballistic missiles and cruise missiles will be faster and more maneuverable to counter defenses."[16] The Hong Kong publication *Chien Shao*, in an article about a newly promoted Political Commissar of the Second Artillery Corps, reported that he was involved with the "speeding up [of] the research and development of the new Dongfeng 51 (DF-51) missile."[17] Other than the designators, there is no publically available information on these missiles.

---

[10] "Taiwan Report on PRC Missile Buildup to Deter U.S. Forces," Taipei *Taipei Times*, May 7, 2001. Transcribed in Open Source Center Doc. ID: CPP20010507000114.

[11] *ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2011*, op. cit. p. 34.: "Defense of Japan 2011," part, 1, page 78, available at: <http://www.mod.go.jp/e/publ/w_paper/pdf/2011/12Part1_Chapter2_Sec3.pdf>.: "Short-range Campaign Tactical Missiles Deployed in Guangdong," Toronto *Kanwa Asian Defense Review Online*, September 1, 2011 Transcribed by Open Source Center Doc. ID: CPP20111103715037.

[12] Ibid.

[13] "BALLISTIC AND CRUISE MISSILE THREAT," NASIC-1031-0985-09, p. 29, available at: <http://www.fas.org/programs/ssp/nukes/NASIC2009.pdf

[14] "Comparison of Missile Strength Between China and Taiwan," Hong Kong *Kuang Chiao Ching*, December 16, 2002. Translated in Open Source Center Doc. ID: CPP200212218000070.

[15] "China, Russia: PRC Navy Status, Development Prospects Detailed," Moscow *Morskoy Sbornik,* August 17, 2003. Translated in Open Source Center Doc. ID: CPP20031120000002.

[16] Richard D. Fisher, Jr. and Bill Sweetman, "Sizing Up China's Military Capability," *Aviation Week*, April 5, 2011, available at: <http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?headLine=Sizing%20 Up%20China%27s%20Military%20Capabilities&storyID=news/dti/2011/04/01/DT_04_01_2011_p32-295855.xml>.

[17] Chin Chien-li, "A Critical Biography of General Peng Xiaofeng, Political Commissar of the Second Artillery Corps," Hong Kong *Chien Shao*, December 1, 2006-December 31, 2006. Translated by Open Source Center Doc. ID: CPP20061215710002.

Retired Russian Colonel and Member of the Russian Academy of Military Sciences Yuriy Sumbatyan wrote that "as many as 500 or 600" of Chinese combat aircraft "are capable of carrying nuclear weapons."[18] Until recently, most of these were relatively short-range aircraft. However, starting in the 1990s, the Chinese began the introduction of Su-27 and Su-30 Russian heavy fighters. Reportedly, China has a regiment of H-6 bombers devoted to the nuclear mission.[19] The large J-20 stealth fighter is an obvious candidate for a nuclear strike system. There are reports from China that it is developing a stealth bomber which is referred to either as the H-8 or the H-10.[20]

Over the past two decades China has continued to develop nuclear weapons. China prepared for the cessation of high-yield nuclear testing by staging a series of underground nuclear tests in the 1990s. Yu Min, described in *Xinhua* as the "architect of the country's first H-bomb," claims that China's key nuclear capabilities are "on a par with the United States and the former Soviet Union."[21] This is clearly an exaggeration, but China appears to be working diligently to close the gap. Xue Bencheng, one of the most important scientists involved in the development of China's neutron bomb, stated that the July 1996 Chinese nuclear test was "a great spanning leap" because it solved the problem of nuclear weapons miniaturization.[2522] Critically China's nuclear weapons technology has been augmented by large scale espionage against the United States. The Chinese nuclear arsenal reportedly includes fairly advanced thermonuclear warheads, enhanced radiation weapons, and other tactical nuclear weapons, including nuclear artillery and antiship weapons.[23]

The House Intelligence Committee concluded that after the declared end of Chinese nuclear testing, "nuclear tests related to development of the PRC's next generation of thermonuclear warheads may be continuing at the PRC test site at Lop Non Nor."[24] In May 2006, *Chinese Defense Today* also reported possible "low yield nuclear tests" after the declared end of testing.

Chinese nuclear doctrine is hidden beneath significant quantities of what I believe is political propaganda, most notably a pledge of "no first use" of nuclear weapons. The two major elements of what they call their nuclear doctrine are: 1) supposed no first use of nuclear weapons and 2) the "self defense counter attack".

---

[18] "Sumbatyan discusses a 'modernizing' People's Liberation Army," Moscow *Voyenno-Promyshiennyy Kuryer*, June 30, 2004. Translated in Open Source Center Doc. ID: CEP20040701000368.

[19] Andreas Rupprecht, "The Dragons' Wings," *Air Combat*, February 2012, p. p. 63.

[20] "Xian H-8 Chinese Stealth bomber," available at:<http://www.grandestrategy. com/2007/11/xian-h-8-chinese-stealth-bomber.html>.: "China's H-10 stealth bomber secret flight - can carry nuclear bomb*," China Arsenal*, December 7, 2009, available at: <http://china-arsenal.blogspot.com/2009/12/chinas-h-10-stealth-bomber-secret.html>.

[21] "PRC Nuclear Weapons Researcher Comments on Development of H-Bombs," Beijing *Xinhua*, December 21, 2005. Transcribed in Open Source Center Doc. ID: CPP20001221000097.

[22]PRC Chief Engineer of Neutron Bomb Interviewed on Nuclear Weapons Development," *Chengdu Sichuan Ribao*, June 11, 2001. Translated in Open Source Center Doc. ID: CPP20010613000011.

[23] "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," available at:<http://www.access.gpo.gov/congress/house/hr105851-html/ch2bod.html# anchor4309987>.

[24] *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of* China, Volume I (unclassified), May 1999, pp. 69-76 and 241.

With regard to "no first use," a careful look at the Chinese wording of China's "no first use" policy reveals that it commits them to nothing.[25] The Pentagon report on the Chinese military states, "there is some ambiguity" over the conditions under which China's "no first use" policy would apply, "including whether strikes on what China considers its own territory, demonstration strikes, or high altitude bursts would constitute a first use."[26] The *Kyodo News Agency* revealed that it obtained classified Chinese documents which say that China "will adjust the nuclear threat policy if a nuclear missile-possessing country carries out a series of air strikes against key strategic targets in our country with absolutely superior conventional weapons…"[27] Chinese generals also threaten nuclear attacks against the U.S. if it comes to the aid of Taiwan.
Significantly, China's Arms Control Ambassador once said that "no first use" does not apply to a conflict over Taiwan. Indeed, Chinese nuclear doctrine has evolved toward "active defense," which implies a nuclear warfighting component.

An interview with Chinese Major General Cai Yuqiu, Vice Principal of Nanjing Army Command College, published in *Ta Kung Pao*, an internet version of a PRC-owned daily newspaper, reported "Cai Yuqiu said that he really appreciated the four sentence fight principle by Mao Zedong, i.e., we will not attack unless we are attacked; if we are attacked, we will certainly counter-attack. As to whether we will use nuclear weapons first, the above principle can also be followed. If we have been repeatedly 'attacked,' then there should not be a limit for our counter-attack."[28] Writing in January 2005, Colonel Wen Shang-hsien of the Taiwan military noted that after the year 2000 the PRC adopted a nuclear doctrine which allowed for 'a preemptive strike strategy' under which the PRC would use "its tactical nuclear weapons in regional wars if necessary."[29] As one Hong Kong newspaper put it, this means that the People's Liberation Army will "launch the first strike when the enemy starts a military buildup or prepares for a strike in order to destroy all possible military targets and war forces."[30]
"Self defense counter attack" is a multipurpose formulation the Chinese use to describe most instances where China has initiated the use of force, which is almost always the case. It is worth noting that China described its 1962 invasion of India as "self defense counter attack".[31] China described its border war

---

[25] "Opinion: The Trouble With China's Nuclear Doctrine," *Jane's Defense Weekly*, February 22, 2006, available at: <http.www.janes.com/defense/news/jdu/jdw060216_1_n.shtml>.
[26] *ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2011*, op. cit. p. 34
[27] "Chinese Military Yes Preemptive Nuclear Attack in Event of Crisis," *Kyodo News Agency*, January 5, 2011, available at: <http://www.profesionalsoldiers.com/forums/showthread.php?t=31796>.
[28] Wu Pin, "Military Scholar on Tactics Views Defense Issue," Hong Kong *Ta Kung Pao Internet Version*, August 1, 2007. Translated in Open Source Center Doc. ID: CPP20070806710004.
[29] Colonel Wen Shang-hsien, "An Investigation into the Impact of the PRC's Use of Nuclear Weapons on both Taiwan and the PRC," Taipei *Ho-sheng-hua Fang-hu Pan-nien-k'an*, January 1, 2005. Translated in Open Source Center Doc. ID: CPP20071030312005.
[30] "'Great Wall Project' Said To Deter Taiwan Independence," Hong Kong *Sing Tao Jih Pao, November 26, 1999.* Translated in Foreign Broadcast Information Service Doc. ID: FTS19991227000170.
[31] Cheng Feng and Larry M. Wortzel, "PLA Operational Principles and Limited War," in Mark A. Ryah, David M. Finkelstein and Michael A. McDevott. *Chinese Warfighting, The PLA Experience Since 1949*, Armonk NY: M.E. Sharpe, 2003, p. 181.:"Sino-India Border Self-Defense Counter-Attack Battle 1962, " *Orbat*, April 7, 2002, available at: <

with the Soviet Union in 1969 as a "self defense counter attack."[32] It also described its 1979 invasion of Vietnam as a "self defense counter attack."[33]

The Congressional Commission on the Threat to the United States from Electromagnetic Pulse (EMP) reported, "China and Russia have considered limited nuclear attack options that, unlike Cold War plans, employ EMP as the primary or sole means of attack."[34] The 2005 Pentagon report on Chinese military power observed, "Some PLA theorists are aware of the electromagnetic effect of using a high-altitude electromagnetic pulse (HEMP), and might consider using HEMP in an unconventional attack, believing that the United States and other nations would not consider it as a use of force and a crossing of the nuclear threshold."[35] A Congressional Research Service report by Ronald O'Rourke concluded that a U.S. naval force coming to the aid of Taiwan against a Chinese attack would have to be prepared for use of nuclear weapons and EMP because "China could also use a nuclear-armed ballistic missile to detonate a nuclear warhead in the atmosphere to create a high-altitude electromagnetic pulse (EMP) intended to temporarily or permanently disable the electronic circuits of U.S. or other civilian and military electronic systems."[36]

Based on my research, I believe China will use nuclear weapons first if they think it in their national interest to do so.

According to the 2004 White Paper of the Chinese Defense Ministry, the "Chinese people and armed forces will resolutely and thoroughly crush it [Taiwan's independence] *at any cost*."[37] (Emphasis added). In the words of Yan Xuetong, Director of the Qinghua University Institute of International Affairs, "so long as China is ready to achieve reunification at all costs, the United States will consider whether it is necessary to support Taiwan at the price of a nuclear war."[38]

We should not mirror image Western views about nuclear weapons onto the Chinese. Indeed, in March 2012 China's official news agency reported, "After being briefed by Liang Xiaojing, an officer from the PLA Second Artillery Corps, [President] Hu said the PLA Second Artillery Corps shoulders missions that are important for the country, and he expected officers like Liang to play an active role in

---

http://orbat.com/site/history/historical/china/sinoindia1962.html>.

[32] Vivian Yang, "Days Without Whites*," Co/ASIS*, available at: <http://www.sunoasis.com/whitestory.html>.

[33] Michael D. Swain and Ashley T. Fellis, *Reinterpreting China's Grand Strategy, Past Present and Future*, Santa Monica: Rand Corporation, 2000, p. 77.

[34] *Report of the Commission To Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Summary*, 2004, available at: <http//.www.globalsecurity.org/wmd/ library/congress/ 2004_r/04-07-22emp.pdf>.

[35] *The Military Power of the People's Republic of China 2005*, Washington D.C.: U.S. Department of Defense, 2005, p. 40 available at: <http://www.defense.gov/news/jul2005/d20050719china.pdf>.

[36] Ronald O'Rourke*, China's Naval Modernization: Implications for U.S. Navy Capabilities – Background and Issues for Congress*, Washington D.C.: Congressional Research Service, November 18, 2005, p. CRS-15.

[37] Xinhua: 'Full Text' of White Paper titled "China's National Defense, 2004," Beijing *Xinhua*, December 27, 2004. Transcribed in Foreign Broadcast Information Service Doc. ID: CPP200412270000034.

[38] Beijing Scholar: China Should Contain Taiwan Independence by Force," Singapore *Lianhe Zaobao*, November 28, 2003. Translated in Open Source Center Doc. ID: CPP20031130000033.

ideological mobilization to prepare for military actions."[39] Ideology is still a major element of Chinese nuclear weapons policy.

Mao's extreme views about the acceptability of hundreds of millions of dead Chinese is still influencing views in China. For example, in 1996, Lieutenant General Xion Guangkai, then a Deputy Chief of the PRC General Staff, made an implied threat to destroy Los Angeles in the event of a conflict over Taiwan.[40] He was also quoted as saying that to prevent Taiwanese independence, "China was prepared to sacrifice millions of people, even entire cities in a nuclear exchange.…"[41] In 2005, Chinese Major General Zhu Chenghu threatened nuclear first use against the United States in which, "We Chinese will prepare ourselves for the destruction of all of the cities east of Xian….Of course, the Americans will have to be prepared that hundreds of cities will be destroyed by the Chinese."[42] No Western military leaders make threats like this. Will the Chinese act on such a basis in a crisis? I can't get into their heads and neither can anyone else.

China is most likely to initiate the use of nuclear weapons if it is being defeated in warfare – such as during a Taiwan scenario or because of the scale of damage from conventional precision guided munitions.

China announced years ago that it was going forward with ballistic missile defense. China's commitment to missile defense was reiterated in the 2010 defense white paper which linked missile defense to its broader strategy of "Active Defense": "The PLAAF [Peoples Liberation Army Air Force] is working to ensure the development of a combat force structure that focuses on air strikes, air and missile defense, and strategic projection, to improve its leadership and command system and build up an informationized, networked base support system."[43] The 2011 edition of the Pentagon report on Chinese military power detailed Chinese missile defense efforts.

China is proceeding with the research and development of a missile defense umbrella consisting of kinetic energy intercept at exo-atmospheric altitudes (>80 km), as well as intercepts of ballistic missiles and other aerospace vehicles within the upper atmosphere. In January 2010, China successfully

---

[39] "Hu Jintao meets PLA officers, professionals," *Xinhua*, March 12, 2012, available at: <http://english.peopledaily.com.cn/90785/7757331.html>.

[40] Patrick Moore, "Asia: China Becoming a Regional Military Threat?" July 22, 2005, available at: <http://www.rferl.org/featuresarticle/2005/07/71c5f120-4cbd-487f-927c-0d0420df09e0.html.>

[41] Quoted in Keith Payne, *The Fallacies of Cold War Deterrence and a New Direction*, Lexington: University of Kentucky Press, 2001, p. 128, available at: <http://books.google.com/books?id =rJ2MD4V84pIC&dq=The+Fallacies+of+Cold+War+Deterrence+and+a+New+Direction&pg=PP1&ots=fjM1veXkKg&sig=3yOJwuK9rFGnEoqo3f5EW0qxdbw&prev=http://www.google.com/search%3Fhl%3Den%26q%3DThe%2BFallacies%2Bof%2BCold%2BWar%2BDeterrence%2Band%2Ba%2BNew%2BDirection%26btnG%3DGoogle%2BSearch&sa=X&oi=print&ct=title#PPP1,M1>.

[42] Jonathan Watts ,"Chinese general warns of nuclear risk to US," *The Guardian*, July 15, 2005, available at: <http://www.guardian.co.uk/world/2005/jul/16/china.jonathanwatts>.

[43] *"Full Text: China's National Defense in 2010 (1)," Xinhua: 'Full Text' of China's National Defense in 2010, Beijing Xinhua, March 31, 2011. Transcribed by Open Source Center Doc. ID: CPP20110331968049.*

intercepted a ballistic missile during its mid-course phase of flight, using a ground-based missile.[44] According to Richard Fischer and Bill Sweetman, China is developing, "A new air- and missile-defense interceptor family, sometimes called the HQ-19 (HHQ-26 for the naval version), [which] reportedly has performance goals similar to the 400-km Russian S-400."[45] Longer range radars could upgrade this system into one capable of intercepting ICBMs. In February 2012, the Hong Kong *Wen Wei Po Online*, which is owned by the PRC, reported Chinese interest in buying the Russian S-400 and quoted "Hong Yuan, a famous military science scholar in Beijing" to the effect that "possessing S-400 will play an important role in enhancing China's missile defense and air defense, but as the missile system has not been tested in actual operations, its technical parameters have yet to be verified in contemporary wars."[46] It also reported, "The purchase of S-400 will play an important role in enhancing China's missile defense and air defense power, especially being of high reference significance for intermediate-range to long-range missile defense."[47] There is nothing unusual about the Chinese buying a Russian system and attempting to develop a Chinese counterpart with similar or improved capabilities.

The PRC's nuclear threat is serious not at least because it is in the context of a general military buildup that is aimed at combating the United States and enabling the expansion of Chinese power in the Pacific. With the demise of the Soviet Union, the PRC ceased to face any serious national security threat. China is beginning to throw its weight around and its actions have generated serious security concerns in the Far East. At this moment, Taiwan is not on the front burner but that could change quickly. No other country has increased its military spending by double digits for twenty years with the intent of a "peaceful rise"?

---

[44] *ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2011*, op. cit. p. 32.

[45] Fisher, Jr. and Sweetman, "Sizing Up China's Military Capability," op. cit.

[46] Wang Hsiao-hsueh, "Expert Interpretation: Purchase of Russian S-400 Missiles Will Enhance China's Missile Defense," Hong Kong *Wen Wei Po Online*, February 27, 2012. Translated by Open Source Center Doc. ID: CPP20120227787011.

[47] Ibid.

CHAIRMAN SHEA: Thank you very much.
Phil.

OPENING STATEMENT OF DR. PHILLIP C. SAUNDERS
DIRECTOR, CENTER FOR STUDY OF CHINESE MILITARY AFFAIRS
NATIONAL DEFENSE UNIVERSITY

DR. SAUNDERS: Thank you for the opportunity to testify today.

I do direct the Center for the Study of Chinese Military Affairs at NDU, but what I'm going to say today are my own personal views, not those of NDU, the Department of Defense or the administration.

I think it's worth starting why does China have nuclear weapons? They felt they had a lot of political value. They felt they had been vulnerable to U.S. nuclear blackmail in multiple instances, and as Mao Zedong put it, "what others have, we must have."

So they do feel there's value to them, but primarily in countering nuclear attack, in countering, in deterring nuclear attack and countering coercion. And having nuclear weapons does raise a state's status, but there isn't much in Chinese writings that says anything about numbers mattering a lot or a larger force really conveying prestige or other benefits.

And they seem to believe that one or a very few nuclear weapons striking somebody's homeland is enough to achieve strategic deterrence.

People often talk about China's nuclear strategy as a minimal deterrent focused on a small number of weapons to deliver punitive counter value responses to an adversary's first strike. As you parse that out, that means the lowest number of damage necessary to prevent attack--a few missiles.

This started out as something that's technologically driven in terms of China only having a limited first air-delivered capability and then very crude ICBM capability so there were technological constraints.

But there was also political guidance given, especially by Mao Zedong, which has continued to shape both the formal policy but more to the point the operational doctrine and the campaign planning that the Second Artillery, in particular, uses instead.

You've had some of the comments on the White Paper. I guess I would not agree with dismissing it. I think it does present some of the basic principles, and just to paraphrase: the goal of deterrence and preventing nuclear coercion; a no-first use policy; the goal of eventual elimination of weapons; and a determination not to engage in nuclear arms races.

And if you parse those things out, they don't necessarily dictate a

precise force structure. I would argue that they are relative, and it's relative to what an adversary has, and that's how you have to think about it. So what does a "lean and effective nuclear force" talked about in the White Paper mean, how you translate that into force posture, it's not clear.

But I think about it and Chinese writings think about it in terms of a survivable force, one that can survive a nuclear first strike through some combination of mobility, dispersal, camouflage, operational resilience, tunneling, as you heard in the last section, and then be able to launch a big enough retaliatory strike to penetrate defenses and inflict unacceptable damage.

So if you think about what it means, it depends significantly on what a potential adversary's intelligence, conventional precision strike, nuclear strike, and anti-submarine capabilities and missile defense capabilities are. So it's a relative thing, and you have to think about it that way.

Ambiguity does play a role, especially in the early days of China's deterrence. They felt their deterrence rested on an adversary not being able to be sure you could get all of China's weapons. So ambiguity does play a significant role. I would say that's somewhat true with ICBMs. It's a lot more true with shorter range systems, and, in particular, in the '70s and '80s, we really didn't have much of a clue whether they had tactical nuclear weapons. They clearly did because they dropped some from an airplane, but whether they were in the force, if you look at the declassified estimates, it's just not clear.

Where they are now is modernizing from a first generation force of cave and silo-based ICBMs to a second generation force that is solid-fueled, that is mobile, that's much more survivable, and as was mentioned, looking even forward to a third generation force that may be mobile and MIRVed, which requires a much smaller nuclear warhead to get there.

I think our best hard information on this, which is informed by classified U.S. government analysis, is the Pentagon China Report which talks in terms of ICBMs, in 2010, of about 21 first generation, about 30 second generation, and in 2011, of 55 to 65 ICBMS.

There is also modernization of the nuclear submarine force. The first submarine is ready. The missiles have had some problems in the testing and delivery of it, and so you're looking at that as something that's not quite ready to come on line, but probably a force of at least two to five submarines. Those will carry two SLBMs each, and if you add that up, it's a significant expansion of the number of ICBMs that can hit the U.S.

There are also regional forces, but I won't dwell on them. And I think you're seeing qualitative improvements as well, including a lot of efforts to penetrate U.S. missile defenses. We can talk about that later if you would like.

A key question is, okay, I talked about the policy, I talked about the force structure, is this consistent with their doctrinal materials; is it consistent

with their training? That's what we have to look at to judge this, and I think the best analysis of this, including looking at Science of Second Artillery Command Campaigns, which is classified as a top secret Chinese document, finds that there is a lot of compatibility there with what the stated principles are and with what the training is.

They're training in an environment that they assume there has been a nuclear strike. They're training to survive in that kind of environment, and it does seem fairly consistent, and one key finding from the academic literature is that a lot of the guidance, the political guidance, still seems to apply and be consistent with this doctrine.

I think there are concerns about the no-first use piece of this, not so much that the training is inconsistent, but that they worry, for example, about a conventional strike on their nuclear arsenal, and I think you've seen Chinese military officers try to create ambiguity there.

There have been broader debates within China about whether they ought to revise or abandon that officially, a debate in the mid-'90s about whether to move toward a nuclear warfighting doctrine. At the end of the day, that was rebuffed, and they did not change their policy.

Another debate in 2005 and 2006 about this issue of conventional strikes and missile defenses, did they need to move off that no-first use doctrine, and, again, the answer after a big internal debate was no.

So I think that is an issue where there is some ambiguity. A couple more points to make is there's a tension between this no-first use doctrine and a retaliatory doctrine, and what we see in Chinese doctrine about the importance of maintaining the initiative.

And that's definitely a tension that's there both in conventional campaigns and to some degree in the nuclear side as well. We talked about the force, but if they MIRVed the DF-5, if they come up with a follow-on missile that is MIRVed, given the small numbers, does that create crisis instability? And as you move to a mobile force, especially a submarine-based force, what are the issues with safety and survivability or safety and preventing unauthorized launches? I think that becomes a question.

Right now, they separate the warheads from the missiles. It's pretty hard to launch and make it go boom if you don't have the nuclear warhead on board. That's not probably going to be possible with the nuclear weapons deployed on a submarine.

And then a final point about knowledge and what we know and how we know it. A lot of what we know is from publicly-articulated policies, study of doctrinal materials, and in the open source world, declassified intelligence analysis and U.S. government open reports that are informed by that analysis.

But there is one key thing that we don't know a lot about, which is

how do China's civilian leaders really think about it? We can read the military writings, and we do. We can look at the doctrine, which is approved, at least at some level, by civilian leaders, but we don't really know how China's civilian leaders who don't have a lot of military experience, who aren't taught about nuclear doctrine in the Central Party school, we don't know how they really think about nuclear weapons today or whether the elaborate doctrine and thinking about it, whether that would really go over and be persuasive in the event of a crisis.

Let me stop there. Thank you.

PREPARED STATEMENT OF DR. PHILLIP C. SAUNDERS
DIRECTOR, CENTER FOR STUDY OF CHINESE MILITARY AFFAIRS
NATIONAL DEFENSE UNIVERSITY

March 26, 2012

Dr. Phillip C. Saunders
Director, Center for the Study of Chinese Military Affairs
Institute for National Strategic Studies
National Defense University

Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "Developments in China's Cyber and Nuclear Capabilities"

Dr. Saunders is speaking in his own personal capacity as a member of the academic community. This statement represents his views based on his research. It should not be implied to represent the views of the Department of Defense or the Administration.

Chinese Nuclear Forces and Strategy

China's initial quest for a nuclear weapons capability was motivated by recognition of the political value of nuclear weapons and by Mao Zedong's determination to remove China's vulnerability to nuclear blackmail, which had been a factor in several crises involving the United States.[1] China's senior political and military leaders have consistently emphasized that the principal utility of nuclear weapons lies in deterring a nuclear attack and countering nuclear coercion.[2] Although Chinese leaders believe that possession of nuclear weapons bestows international status, they do not believe that more warheads increase a state's power or status. Unlike U.S. and Soviet strategists who focused heavily on the potential impact of relative capabilities in nuclear war-fighting scenarios, Chinese leaders appear to have concluded that one or a few nuclear weapons striking an adversary's homeland would constitute unacceptable damage, making a large arsenal unnecessary to achieve the desired strategic effects. Following its first nuclear test in 1964, Beijing announced that it would adhere to a policy of no-first-use (NFU) of nuclear weapons and called for worldwide nuclear disarmament. It has maintained this official positions ever since.

---

[1] John Wilson Lewis and Xue Litai, *China Builds the Bomb* (Stanford: Stanford University Press, 1988); Zhang Shu Guang, *Deterrence and Strategic Culture: Chinese-American Confrontation, 1949-1958* (Ithaca: Cornell University Press, 1992). On U.S. nuclear threats to China, see Gordon H. Chang, "To the Nuclear Brink: Eisenhower, Dulles, and the Quemoy-Matsu Crisis," in Sean M. Lynne-Jones, Steven E. Miller, and Stephen Van Evera, eds., *Nuclear Diplomacy and Crisis Management* (Cambridge, Mass.: MIT Press, 1990), pp. 200-227.

[2] M. Taylor Fravel and Evan S. Medeiros, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure," *International Security*, Vol. 35, No. 2 (Fall 2010), pp. 48–87.

Western analysts have described China's nuclear strategy as a "minimal deterrent" that relies on a small number of nuclear weapons to deliver punitive, counter-value responses to an adversary's first strike.[3] Minimum deterrence refers to "threatening the lowest level of damage necessary to prevent attack, with the fewest number of nuclear weapons possible."[4] China's choice of minimal deterrence was influenced by technological constraints on its nuclear arsenal and delivery systems, but was also heavily shaped by the views of senior political leaders (especially Mao), which have had an enduring influence on PRC nuclear doctrine. Chinese leaders did not dictate a specific number of nuclear weapons; China's nuclear forces appear to have been sized based on the need for a few weapons to survive a first strike and launch a retaliatory attack.

China's 2006 Defense White Paper provides a concise overview of the key elements of China's "self-defensive" nuclear strategy:

> Its fundamental goal is to deter other countries from using or threatening to use nuclear weapons against China. China remains firmly committed to the policy of no first use of nuclear weapons at any time and under any circumstances. It unconditionally undertakes not to use or threaten to use nuclear weapons against non-nuclear-weapon states or nuclear-weapon-free zones, and stands for the comprehensive prohibition and complete elimination of nuclear weapons. China upholds the principles of counterattack in self-defense and limited development of nuclear weapons, and aims at building a lean and effective nuclear force capable of meeting national security needs. It endeavors to ensure the security and reliability of its nuclear weapons and maintains a credible nuclear deterrent force. China's nuclear force is under the direct command of the Central Military Commission (CMC). China exercises great restraint in developing its nuclear force. It has never entered into and will never enter into a nuclear arms race with any other country."

This description highlights a number of key elements of China's nuclear strategy and policy, including the goals of deterrence and preventing nuclear coercion; "no-first use" policy; the goal of eventual elimination of nuclear weapons; and China's explicit determination (which dates from the beginning of its nuclear weapons program) not to engage in nuclear arms races.

In terms of doctrine, a no-first use policy implies an operational focus on retaliatory counter-attack, or "striking after the enemy has struck." In terms of force structure, "limited development of nuclear weapons" and a "lean and effective nuclear force" do not translate directly into requirements for specific numbers of nuclear weapons and delivery systems. Rather, they suggest that the quantitative

---

[3] Avery Goldstein, *Deterrence and Security in the 21st Century: China, Britain, France, and the Enduring Legacy of the Nuclear Revolution* (Stanford, Calif.: Stanford University Press, 2000); Jeffrey Lewis, *The Minimum Means of Reprisal: China's Search forSecurity in the Nuclear Age* (Cambridge, Mass.: MIT Press, 2007); and Litai Xue, "Evolution of China's Nuclear Strategy," in John C. Hopkins and Weixing Hu, eds., *Strategic Views from the Second Tier: The Nuclear Weapons Policies of France, Britain, and China* (San Diego: University of California Press, 1994), pp. 167–190. Phillip C. Saunders and Jing-Dong Yuan, "China's Strategic Force Modernization," in Albert Willner and Paul Bolt, eds., *China's Nuclear Future* (Boulder, Col.: Lynn Rienner, 2006), pp 79-118.

[4] Committee on the U.S.-Chinese Glossary of Nuclear Security Terms, *English-Chinese, Chinese-English Nuclear Security Glossary* (Washington, D.C.: National Academies Press, 2008), p. 36.

requirements for a "lean and effective" nuclear force will depend on the ability of Chinese nuclear forces to survive a potential adversary's nuclear first strike via some combination of mobility, dispersal, camouflage, and operational resilience and then to launch a retaliatory strike that can penetrate an adversary's missile defenses and inflict unacceptable damage. Chinese nuclear force requirements thus depend significantly on the intelligence, conventional precision-strike, nuclear strike, anti-submarine warfare, and missile defense capabilities of potential adversaries. China's nuclear forces are not solely focused on the United States, but U.S. capabilities (and potential future advances) in these areas make it a key driver of Chinese force structure.

The development of China's nuclear forces is broadly compatible with the thinking of Chinese top political leaders (especially Mao and Deng) described above. Technological limitations meant that the Chinese deterrent initially relied primarily on air-delivered weapons and then on vulnerable silo and cave-based missiles. Chinese experts privately admitted that the credibility of China's deterrent rested on a potential adversary's uncertainty about whether a first strike could destroy all of China's long-range nuclear missiles. Ambiguity about the total size of China's nuclear arsenal was therefore viewed as an important element of China's deterrent capability. Rather than build large numbers of highly vulnerable first-generation missiles, China decided in the late 1970s and early 1980s to develop a second generation of mobile land and sea-based missiles that would be more survivable and better able to provide a credible second-strike capability. As these new systems began nearing deployment in the late 2000s, U.S. withdrawal from the ABM treaty and deployment of ballistic missile defenses challenged the premises behind mutually assured destruction, prompting Chinese complaints that the United States sought "absolute security" for itself while keeping others vulnerable.

China's current nuclear forces consist of a mix of first and second generation nuclear missiles, with new DF-31 and DF-31A solid-fueled mobile Intercontinental Ballistic Missiles (ICBMs) gradually being deployed to augment existing DF-5A ICBMs. China has also upgraded its regional nuclear deterrent with the deployment of the DF-21 Medium-Range Ballistic Missile (MRBM) to supplement first generation DF-3 and DF-4 Intermediate-Range Ballistic Missiles. In terms of a sea-based deterrent, China's initial XIA class nuclear missile submarine (SSBN) suffered from a troubled development process and may never have constituted a truly operational system.[5] China has already built two Type-94 JIN class SSBNs and may ultimately deploy five of the submarines, which will be equipped with JL-2 SLBM missiles.[6]

The interaction between evolving U.S. military capabilities and China's nuclear modernization is likely to produce a significant expansion of the number of deployed warheads that can reach the United States. However, it is difficult to speak about the numbers with confidence because China provides no official data on the current or projected size of its nuclear force, the number and capabilities of its delivery systems, or its overall modernization plans. A 2010 Pentagon report estimates that China's current ICBM arsenal consists of approximately 20 first-generation ICBMs and approximately 30 solid-fueled,

---

[5] John Wilson Lewis and Xue Litai, *China's Strategic Seapower: The Politics of Force Modernization in the Nuclear Age* (Stanford, Calif.: Stanford University Press, 1994).

[6] Office of the Secretary of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China, 2010.

road-mobile second-generation ICBMs. China's future nuclear forces are likely to include additional second-generation ICBMs and possibly upgrades to allow its first generation ICBMs to carry multiple warheads.[7] The 2011 report gave an updated estimate of 55-65 ICBMs and also noted that "China may also be developing a new road-mobile ICBM, possibly capable of carrying a multiple independently targetable re-entry vehicle (MIRV)."[8] The Pentagon report also notes that "the first of the new JIN-class (Type 094) SSBN appears ready, but the associated JL-2 SLBM appears to have encountered difficulty, failing several of what should have been the final round of flight tests. The date when the JIN-class SSBN/JL-2 SLBM combination will be operational is uncertain."[9]

Most observers expect these modernization efforts to produce both a quantitative expansion in the number of Chinese ICBMs and SLBMs that can reach the United States and qualitative improvements in the capabilities of Chinese missiles. The Pentagon report also notes that China is developing "a range of technologies to attempt to counter U.S. and other militaries' ballistic missile defense systems, including maneuvering re-entry vehicles, MIRVs, decoys, chaff, jamming, thermal shielding, and anti-satellite (ASAT) weapons. PRC official media also cites numerous Second Artillery Corps training exercises featuring maneuver, camouflage, and launch operations under simulated combat conditions, which are intended to increase survivability. Together with the increased mobility and survivability of the new generation of missiles, these technologies and training enhancements strengthen China's nuclear deterrent and enhance its strategic strike capabilities."[10]

China's nuclear arsenal has remained relatively small, consistent with China's nuclear strategy, even as some of the technical constraints on building a larger, more sophisticated nuclear arsenal have eased. But are China's nuclear doctrine and the Second Artillery (the branch of the PLA that controls China's ground-based nuclear forces) training consistent with the publicly articulated strategy? Although the official campaign outlines and combat regulations for China's nuclear forces are classified documents inaccessible to Western scholars, enough internal doctrinal materials have become available to permit an assessment. Broadly speaking, these doctrinal materials and published reports about Second Artillery Corps training are consistent with Chinese public statements about nuclear strategy such as the white paper quoted above.

The 1987 volume *The Science of Military Strategy* identifies key doctrinal principles addressing the deterrent and retaliatory uses of nuclear weapons.[11] The book also emphasizes the concept of "effectiveness" and highlights survivability as a key component of an effective nuclear deterrent. Subsequent editions and other doctrinal materials retain this emphasis, demonstrating that the principles

---

[7] Ibid, p. 34.

[8] Office of the Secretary of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China, 2011, p. 34 and 3.

[9] Office of the Secretary of Defense, Military and Security Developments Involving the People's Republic of China, 2010, p. 34.

[10] Ibid, p. 34.

[11] The four principles are centralized control (*jizhong zhihui*), strike only after the enemy has struck (*houfa zhiren*), close defense (*yanmi fanghu*), and key point counter-strikes (*zhongdian fanji*). *The Science of Military Strategy* [*Zhanlue Xue*] (Beijing, Academy of Military Sciences, 1987), cited in Fravel and Medeiros, 69.

originally articulated by Mao and Deng have continued to guide initial Chinese nuclear strategy and campaign planning even as technical and resource constraints on development of advanced nuclear forces have eased. For example, doctrinal materials published in the early 2000s describe the Second Artillery's "nuclear counterstrike campaign" and refer to "striking after the enemy has struck" as a basic guiding principle.[12] This is consistent with China's "no first use" policy as well as with open source materials on Second Artillery training, which stress the need to be prepared to operate in an environment where nuclear strikes have occurred.

Another distinctive aspect of Chinese nuclear thinking worth highlighting is the concept of counter nuclear deterrence. This is described as "an operation used to demonstrate China's resolve and will to use nuclear weapons in response to efforts by adversaries to coerce China with nuclear threats."[13] Counter-deterrence operations involve efforts to communicate China's will and resolve to respond to a nuclear attack in order to signal that China cannot be coerced by nuclear threats and to reinforce deterrence. They can be considered a form of nuclear signaling.

Internal debates within the Chinese nuclear community have periodically challenged these principles. One debate in the early 1990s concerned the possibility of a shift to a limited nuclear deterrent that envisioned a broader mix of nuclear capabilities that would support nuclear war-fighting. However this debate concluded by reaffirming the deterrence and counter-coercion principles that had historically guided Chinese nuclear strategy.[14] A later debate in 2005-2006 questioned whether a no-first-use policy was viable given U.S. advances in conventional precision-strike capabilities (which might threaten Chinese nuclear missiles with conventional strikes) and missile defenses (which might be capable of intercepting retaliatory strikes by a limited number of Chinese ICBMs that survived a conventional first strike). Although China did not modify its official description of its "no first use" policy, subsequent statements by officials and military officers created a degree of ambiguity about whether a conventional strike against Chinese nuclear assets or command and control systems constituted a "first use" that justified nuclear retaliation.[15]

Chinese debates about no-first-use highlight Beijing's pursuit of a no-first-use pledge from the United States, a consistent theme in its diplomacy. Chinese officials argue that a no-first-use commitment would help prevent nuclear war, strengthen the non-proliferation regime, and promote nuclear disarmament. They also argue that U.S. conventional superiority means that the United States does not need a first-use option. A U.S. bilateral no-first-use pledge would imply acceptance of Chinese principles about the limited role of nuclear weapons and symbolize an equal, non-hostile political relationship between the two sides. China might hope that a U.S. no-first-use pledge would call U.S. security commitments to its regional allies (the nuclear umbrella) into question, thus potentially

---

[12] Fravel and Medeiros, 76.

[13] Michael S. Chase and Evan Medeiros, "China's Evolving Nuclear Calculus: Modernization and Doctrinal Debate," in James Mulvenon and David Finkelstein, eds., *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army* (Arlington, VA; CNA, 2002), p. 133.

[14] Alastair Iain Johnston, "China's New 'Old Thinking': The Concept of Limited Deterrence," *International Security*, Vol. 20, No. 3 (Winter 1995/96), pp. 5–42.

[15] Fravel and Medeiros, 79-80.

weakening U.S. alliances. The value of such a U.S. pledge would increase significantly if the conventional military balance in the Western Pacific tipped in China's favor. Finally, given that the Chinese conception of deterrence implies coercion as well as restraint, a no-first-use pledge would make it harder for U.S. policymakers to threaten nuclear escalation in a crisis and provide China with the moral and political high ground to resist any such threats.

Although Chinese nuclear doctrine, force structure, and training appear broadly consistent with publicly articulated Chinese nuclear policy, some aspects have raised concerns for Western analysts. One is the emphasis in Chinese military doctrine of the importance of maintaining the initiative, a concept in tension with the retaliatory principle of "strike only after the enemy has struck." Some Chinese military writers argue that this can justify pre-emptive attacks under some circumstances, such as in cases where China has credible early warning of a pending nuclear attack. Chinese doctrinal materials emphasize the potential for nuclear counterstrikes to shock an adversary into submission in the hopes of de-escalating a conflict, and discuss retaliatory attacks against a range of counterforce, countermilitary, and countervalue targets.[16] Another issue involves the challenges that mobile ICBMs and especially SLBMs may pose for command and control of China's nuclear arsenal, especially since their technical advantages may erode traditional controls against unauthorized launches (such as the separation of missiles and warheads in China's older ICBMs). Some analysts worry that China's potential deployment of missiles with multiple warheads may create incentives for first strikes that could be destabilizing in a crisis.[17] Finally, some see the potential for greater PLA influence over nuclear doctrine to move China in the direction of nuclear war-fighting strategies and a larger nuclear arsenal.[18]

A final consideration is that much of what we know about Chinese nuclear policy and strategy comes from publicly articulated policies (such as the section of the 2006 white paper quoted above) or study of doctrinal materials (which reflect PLA writings). We know little about what China's top civilian leaders in the Politburo Standing Committee—the actors who would decide whether China should employ nuclear weapons—think about the employment of nuclear weapons or the role of nuclear weapons in crisis situations. The fact that these leaders have little military experience and have likely not been exposed to academic thinking about nuclear weapons (and nuclear dangers) may be grounds for additional concern.[19] At the end of the day Chinese leaders, like other leaders in other countries, are acutely aware of China's vulnerability to nuclear attack and are likely to be cautious in situations with the potential to escalate to an exchange of nuclear weapons.

---

[16] See sources cited in Fravel and Medeiros, 76-77.

[17] Saunders and Yuan; Michael S. Chase, Andrew S. Erickson, and Christopher Yeaw, "Chinese Theater and Strategic Missile Force Modernization and Its Implications for the United States," *Journal of Strategic Studies*, Vol. 32, No. 1 (February 2009), pp. 67–114.

[18] Mark Schneider, "The Nuclear Doctrine and Forces of the People's Republic of China," *Comparative Strategy*, Vol. 28, No. 3 (July/August 2009), pp. 244–270; and Larry M. Wortzel, *China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, and Campaign Planning* (Carlisle, Pa.: Strategic Studies Institute, U.S. Army War College, May 2007).

[19] The author's interviews with relevant faculty members at the Central Party School suggest that nuclear deterrence is not taught in the international relations and security lectures that senior party members receive.

PANEL III: QUESTIONS AND ANSWERS

HEARING CO-CHAIR WORTZEL: Commissioner Fiedler.

HEARING CO-CHAIR FIEDLER: This morning General Cartwright sort of quietly raised the question again of who was in control of the military, there having been some question in the ASAT test and in a couple of other incidents, stealth, the revelation of their stealth airplane.

It seems to me that it's a greater concern in terms of control of nuclear weapons. What do we know about the control of their nuclear weapons? What do we know about the Central Military Commission's role and the civilian role, party role, in that?

DR. SCHNEIDER: Well, the--

HEARING CO-CHAIR FIEDLER: Let me just add, it seems to me that the political commissar in their structure in the Second Artillery and other nuclear armed forces becomes more critical in that discussion.

DR. SCHNEIDER: Yes, I mean the organization chart is the Central Military Commission, and they're more into collective decision-making at that level than we are, and I believe the military is more powerful and more autonomous than they would be in the United States for the simple reason that they keep the regime in power.

Absent the military, they have no legitimacy. In China, that's one of the reasons they're pushing nationalism rather than communism in China today. In terms of the actual control of nuclear weapons, certainly the unit commander and the political commissar, who is extremely powerful in the Chinese military, play the key role.

They don't have, because of the nature of their nuclear weapons, as Danny Stillman, former Chief of Intelligence at Los Alamos, put it, he said their weapons are not 1. safe, and that's probably the reason that they don't mate them to missiles constantly because that means if something goes wrong, and you drop the weapon or a bullet hits it or there's a fire, you could get a low order accidental nuclear detonation.

So there is no, very little risk of, you know, somebody just turning some keys and doing an unauthorized launch there for a lot of reasons.

I wish we knew more about the high level Chinese decision-making, but, you know, there are limits to our understanding of virtually everything associated with their military.

The Science of the Second Artillery Campaign, and I'm sorry to say it's not a top secret Chinese document; it's an officer training manual.

DR. SAUNDERS: It's not the internal, full internal guidance, but it is marked "top secret."

DR. SCHNEIDER: No. That's not what that is. I mean it's an officer

training manual. It has confidential in it. There are unclassified Western translations of it because basically they're easy to get because there are so many of them printed. And they, I mean they indoctrinate their officers. I mean you do not take the initiative. You only operate on the authority of the Central Military Commission for a launch order, and I think that's central to the way they control nuclear weapons. So it's a combination of the several factors that have that effect.

HEARING CO-CHAIR FIEDLER: Dr. Saunders.

DR. SAUNDERS: I mean I think it's broadly correct that it's the unit commander and the political commissar. There's a lot of emphasis on political--

HEARING CO-CHAIR FIEDLER: That's after they receive orders.

DR. SAUNDERS: That's after they receive orders, but, or it's also to make sure they don't do anything without orders. At the top level, we think it would be, have to be a decision by, not by the Central Military Commission but by--

HEARING CO-CHAIR FIEDLER: Politburo.

DR. SAUNDERS: --Politburo Standing Committee, the top nine senior civilian leaders of the Party. That would be regarded as a very, very serious thing, and it wouldn't be a military decision. Indeed, there are no military officers on the Politburo Standing Committee. Certainly, they would get military inputs and they would get a military perspective on that decision, but at the end of the day, it would be the civilians at the top of that structure who would make a decision whether or not to use nuclear force.

And I touched on the issue of--the de-mating is certainly something, but you can't really do that on a sea-launch ballistic missile. And I think one of the questions there that we just don't know about is what other, do they have technical provisions to make those missiles safe to have a two-man rule or other provisions? They've been exposed to some of that technology, but I don't think we know for sure the extent to which they may have adopted it.

HEARING CO-CHAIR WORTZEL: Just to end the discussion that looks like it was brewing between you guys, I've seen the inventory of the Science of Second Artillery Campaigns at a couple of PLA bookstores. It's published in several versions. Internal distribution only, secret and top secret, so you could have any one of those versions circulated.

Commissioner Wessel.

COMMISSIONER WESSEL: Thank you, gentlemen.

Help me if you can. I want to try and connect in some ways what we heard this morning. We've been increasingly discussing over past years asymmetric warfare and the increasing utilization of cyber activities by the Chinese to enhance their capabilities.

The flip side of that is certainly the U.S. is looking at how it may

utilize cyber activities where there is a potential conflict. With the no-first use doctrine not necessarily being defined as we would always define it here, do you think there is a tipping point for the potential use of cyber activities by the U.S. or some other nation to result in a dramatic engagement by the Chinese?

DR. SCHNEIDER: You mean a tipping point in terms of nuclear escalation?

COMMISSIONER WESSEL: Correct.

DR. SCHNEIDER: I don't really think so. The material I've seen in the doctrinal writings where they talk about adjusting the threshold and going first relate to conventional attacks on China, devastating, very destructive or very effective conventional attacks.

They have, I mean I'm no expert on their cyber capability, but I believe it's absolutely clear they've got extremely sophisticated cyber capabilities, and they would probably use them very extensively in any war against the United States.

I don't believe that they're--I can't say for sure, but I don't believe that there's a big nuclear linkage to cyber warfare, but they would probably win that conflict the way they're developing their capability.

COMMISSIONER WESSEL: No, but do you believe that if we were to engage in dramatic utilization of cyber activities against them that they would escalate? I thought I heard earlier was, no, you don't see it getting to that point.

DR. SCHNEIDER: You mean with the political context there's a war going on?

COMMISSIONER WESSEL: I'm sorry?

DR. SCHNEIDER: Is a war going on?

COMMISSIONER WESSEL: Well, definition of what is a war going on at that point, a conflict, first starting with cyber.

HEARING CO-CHAIR FIEDLER: In other words, if we shut down their electric grid.

COMMISSIONER WESSEL: Correct, correct.

HEARING CO-CHAIR FIEDLER: How would they react?

DR. SCHNEIDER: They engage and, you know, there's a dispute on or uncertainty on who authorizes, but they engage in cyber efforts against, you know, us very frequently. And they've had some great levels of success. I don't see, I see a fundamental break here between the use of cyber operations in peace time and cyber operations in war time.

In war time, it would be a central part of their overall military strategy, and, you know, the outcome of the cyber battle could, I guess, impact significantly the outcome of the war itself.

They are probably most likely to use nuclear weapons if they're losing, if they suffer very damaging attacks, and if the issue is something absolutely

central to them like Taiwan.

DR. SAUNDERS: I just, I would add that, I mean, I think the doctrine that they have on cyber operations or integrated networked electronic warfare does see this as a crucial military capability. It's one that leverages U.S. dependence on computer networks and communications.

Of course, that's also the direction the PLA is going. They're informationizing, they're using computer networks, and systems of systems. So right now we are more dependent and vulnerable. That's going to change over time. But I think they do see this as a warfighting capability and indeed to use one early.

I think the question is what happens if you start doing larger attacks against infrastructure? Both our countries are dependent on cyber to run various parts of our infrastructure and economy. How do you control escalation in that context?

I think one area where there may be linkages with the nuclear side is if you're using cyber attacks against strategic command and control, including nuclear command and control. That starts to get into a very iffy business. Is that a cyber attempt to remove China's nuclear deterrent capability.

COMMISSIONER WESSEL: Neutralize--

DR. SAUNDERS: Is that a first use? I wouldn't say that it is, but it could be seen as an attack on the nuclear capability and that, in my mind, would be extremely dangerous if they tried to do it to us or if we tried to do it to them. So that's a real area to be cautious about.

COMMISSIONER WESSEL: Thank you.

HEARING CO-CHAIR WORTZEL: Dr. Saunders, on page five of your testimony, you have a discussion in the middle paragraph about Chinese doctrine looking at attempts essentially to escalate in order to de-escalate. Nuclear counter strikes to force an opponent to de-escalate.

Now nobody has fought a nuclear war yet, but in nuclear war gaming, when parties escalate to de-escalate, it rarely leads to de-escalation and invariably results in a larger exchange. So I guess the question is how, (a) how realistic do you think that is; and is escalating to de-escalate volatile? And I'd ask both of you that.

DR. SAUNDERS: What the writings talk about is delivering a severe psychological blow, a fundamental shock that causes the adversary to reassess what kind of war they're fighting and, hopefully, from the Chinese point of view, shock them into realizing this has gotten out of hand.

It's one thing to write that in a doctrinal manual. It's another for it to have that effect in real life. I mean I personally think the Chinese leadership has shown it to be very cautious and risk averse across a range of things, and certainly wouldn't lightly undertake a nuclear strike in the first place.

And then if a nice, you know, a PLA officer, whether they're nice or not, comes in and says, well, now we need to do this much bigger strike, and that will bring the war to the end, I would think at that point, hopefully, before that point, they would get some sharp questions from their civilian leadership, and that's why I highlighted this point, that we don't know a lot about what their civilians think.

We know a fair amount about what their military writes, but if the military presents these options in the middle of a crisis, are the civilians going to say that's all we can do? Are they going to say, what, are you crazy?

That's just an area where we don't have a lot of insight. I mean I would hope, to be honest, that the Chinese are doing their own nuclear war gaming and getting civilians to play in some of that because I think if you participate in some of those games, as I know you have, you find them very sobering, and some of the things that seem very clever when you wrote them theoretically have a very different complexion when you see what happens if you try to put it into practice.

DR. SCHNEIDER: A war, any type of war between two nuclear, major nuclear powers, is a very bad idea, and about 30 something years ago, I was asked to write a paper on nuclear war termination, and I reviewed the entire literature on it, and nobody really had a clue how you would do this.

Now, basically, what concerns me most right now, this involves both Russia and China, is the talk in Russia, both military and civilian leadership, about using nuclear weapons, and China, it's mainly the--well, it's entirely, I would guess, the military leadership although this morning by some strange coincidence I found the article which quoted the Deputy Chairman of the Central Military Commission concerning about using nuclear weapons in response to conventional attacks.

Now, but having said that, I fully agree that they're going to be very cautious about using nuclear weapons. What scares me more than anything else is the Taiwan issue because there's nothing like it anywhere in the world. I mean when you combine that with the talk about paying any price, that's kind of scary, and that issue could get out of control. If one election in Taiwan goes the wrong way, you could be back in a crisis situation.

So I mean, and that's one of the reasons I'm also concerned about whether or not if they have tactical nuclear weapons, for example, anti-ship nuclear weapons, which is mentioned in some of their literature, we know they have the DF-21D, which the Pentagon report says it's nuclear armed, and Chinese sources say the same thing, but I'm talking about things like anti-ship cruise missiles, you know, nuclear artillery, potentially other types, nuclear land mines, potentially other types of tactical nuclear weapons, if they use something like that, we have no comparable response.

I mean our forces are not exactly well-designed to deal with limited nuclear strikes or chemical or biological strikes because we've basically reduced it to strategic planned attack systems, and that's not the way--I mean I'm not sure you can control a nuclear war, but I certainly don't think you ought to go about it that way.

HEARING CO-CHAIR WORTZEL: Thank you.

Commissioner Blumenthal.

COMMISSIONER BLUMENTHAL: Thank you. Thank you, both, for your testimony.

I want to turn--somebody quoted Stalin before, and I want to quote Lenin in terms of what is to be done. There's obviously an abstract quality to all of this, which is good. We haven't actually been toe to toe with the Chinese.

With the Soviets, the thresholds and modicums of strategic stability were always--there's a lot of revisionism now, but they're always very near-run things, you know, and strategic stability came after possible nuclear crises and even talk of preemption by the United States, people don't care to remember, and nuclear threats, and so on and so forth, and stability, in the end, what people call stability came with the fact that neither of us had a first-strike option. So people called it strategic stability in that setting, but again that was after years of testing, and very near-run things, and the Cuban missile crisis and elsewhere.

Well, what is deterrence here in terms of our posture and what is strategic stability? I mean so for the Chinese I can understand why they're doing what they're doing. I mean we're talking about things like prompt global strike for which I think we're outfitting all of two missiles, but still, you know, we're talking about prompt global strike.

We're openly talking about attacking in-depth now, not that we have the forces to do it, but we're openly saying that that's part of our air-sea battle concept. We're going to take it to the mainland conventionally. If I was Chinese, I would certainly be interested in nuclear weapons.

So we're so far from stability, I think, so I'd first like to ask the question about deterrence, and, second, in terms of what we should be doing, and second, how do you get to stability?

Silence.

HEARING CO-CHAIR FIEDLER: Don't all jump.

[Laughter.]

DR. SCHNEIDER: My view of the situation in regard to China is essentially this. With the demise of the Soviet Union, China was in a very desirable position. I mean it really faced no, no threats of attacks, yet, in response to that, it began a large expansion of its military capability. I think if, as its power grows relative to ours, and I think that's what the situation is going to be, we'll be in an increasingly dangerous situation that they may try to throw

their weight around in some way. And if they do that, things could get out of hand. You know, the near-term flashpoint is Taiwan.

COMMISSIONER BLUMENTHAL: Yeah. So what do we do? I mean I know all that already. I mean--

DR. SCHNEIDER: Well, I think we need to be spending more money on some elements of our defense posture than we are now. We've got to, well, if you take a look at what was planned in the Clinton administration for today and what we actually have, there is almost no correlation.

COMMISSIONER BLUMENTHAL: Well, how would you do nuclear deterrence?

DR. SCHNEIDER: Oh, nuclear deterrence. I don't think it's wise to do unilateral cuts. I think you want to maintain as much as a margin of superiority over China as is possible for the simple reason that no American president is going to initiate the use of nuclear weapons under any circumstances other than a WMD attack of substantial proportions, whether it's nuclear or whether it's chemical or biological. I'm talking about something that's going to kill hundreds of thousands or millions of people.

I'm less certain about what the Chinese would do in a Taiwan scenario if they actually lost, and keep in mind, invading Taiwan is something like the invasion of Normandy, and it could fail. I mean even with all the money they're putting into their military build-up, it's a very, very difficult situation, and under those circumstances, they just might do it because I think they see regime survival over that issue.

COMMISSIONER BLUMENTHAL: So it's nuclear supremacy for the United States.

What about you, Phil?

DR. SAUNDERS: Well, I think they've committed to having a survivable second-strike capability, and I don't think we can stop them from doing that. So that's a starting point, but they have money, they have the technology, they have enough fissile material. It is rocket science, but it's rocket science where to do it to a certain degree is good enough to produce deterrence.

So I think on the nuclear side, we certainly have a lot more warheads and delivery systems than they do, but it doesn't matter. It takes, all it takes is one nuclear bomb to ruin your day.

COMMISSIONER BLUMENTHAL: Yeah.

DR. SAUNDERS: So I think that's sort of the situation we're in. I don't see how we get out of that. So at that level, sort of a formal level, there is a certain stability. There is a certain degree of mutual deterrence. The question is, is that good enough? We have political problems in the relationship. We have security disputes within Asia. We have the issue of Taiwan. We have concerns about cyber and counterspace capabilities. So there's a lot more going on in the

relationship there that sort of colors it. But at the fundamental level of the nuclear capability, I think that is a pretty stable deterrent relationship.

If we come down in the context of negotiations with the Russians, at some point there has to be an effort to get China and other nuclear- armed states involved, and part of that is they have to be more transparent about capabilities so we know--

COMMISSIONER BLUMENTHAL: Do you think it's stable in the scenario where, you know--which is canonical now almost, they attack Taiwan, we now attack in-depth, and we're stable in terms of who uses nuclear weapons?

DR. SAUNDERS: Two points on that. First, it's not just the military balance or the nuclear balance or the conventional balance. There are very high economic costs for China if they choose to try to resolve this situation via force, and that is a deterrent on them. It's part of a deterrent, and that's partly why they shifted their policy in favor of deterring independence and working politically for peaceful integration.

So that's just a broader point. If they do launch a conventional attack on Taiwan, I think the ways in which we would have to respond to that are going to be very escalatory. They're building a range of conventional capabilities, which we call anti-access area denial, they call counter-intervention, which raises the costs and risks of us operating close to the Chinese coast. There's a variety of ways we can counter that, but one of the ways is going after sensors. That means strikes on the mainland, and that means early on in a conflict.

So that's I think a concern for both sides, is you go from zero to 60 very, very quickly in a conventional conflict that involves the U.S. and China over Taiwan, and I think there are real concerns about escalation there. It's a good reason for them never to choose to roll the dice.

COMMISSIONER BLUMENTHAL: Thanks.

HEARING CO-CHAIR WORTZEL: Commissioner Cleveland.

COMMISSIONER CLEVELAND: Dr. Schneider, I heard you say that we shouldn't reduce unilaterally, but I'm wondering do you think the discussions we had with the Russians over our nuclear inventory should be seen through the lens of the Chinese build-up?

DR. SCHNEIDER: Well, yes and no. The yes part is certainly conceptually that makes enormous amount of sense. No question about it. But the no part of it is I don't see any real prospect for arms control solution with China for a very simple reason: you have only two real alternatives in terms of numbers.

You either grant them equality with the United States and Russia, in which case they get to build up for a long period of time, and I think you have zero chance of getting a treaty like that ratified because there is no national security benefit out of it.

Or you get the Chinese to accept sort of something like the Washington-London agreement where you had a ratio of 5:5:3:1.67, something like that. I cannot see the Chinese under any circumstances agreeing to that. They have sought to generally avoid arms control negotiations. I mean they've made any number of statements over the years about what circumstances they would enter arms control.

The circumstances actually happened, and they didn't. I don't see any burning Chinese desire to enter any type of agreement like a new START or the INF Treaty, and I mean the INF Treaty itself is God's gift to China. I mean since we've eliminated all our missiles, you know, they've added 1,500 or whatever the official number is right now. I mean that's a pretty big advantage. I mean it's literally the core of their current approach to warfighting against the United States, and I don't see them giving that up.

COMMISSIONER CLEVELAND: What about Dr. Karber's comment earlier that the United States and Russia reach a point where they argue, and it is some distance away, needless to say, but that they argue that we may have to give up the INF Treaty if we don't see progress on the Chinese front?

DR. SCHNEIDER: The Russians have said that quite frequently. They have made numerous high-level statements starting in the middle of the last decade about how the INF Treaty was a Cold War anachronism, and they wanted to get out of it. What I think they've done, and I have about ten Russian sources, including four reports in one of their official news agencies, that they're developing an intermediate-range ground-launch cruise missile, the R-500.

And if those reports are true, that's a blatant violation of the INF Treaty. And I've seen statements in the Russian press about we've got to pragmatically interpret the, you know, there's generals saying we've got to pragmatically interpret the INF Treaty. You know, I'm a country lawyer, and I don't see pragmatism having much to do with treaty interpretations.

I mean what it means is the plain meaning of the treaty, how it applies in a fact situation. I mean to me that's in the context of those reports, and there are a lot of them, including, as a matter of fact, when Stratfor was hacked, it turns out that they picked up the same reports.

I would like the U.S. government to take a serious look at what's happening there before we do anything else on arms control because that's a really big issue if those reports are true.

COMMISSIONER CLEVELAND: Thank you.

HEARING CO-CHAIR WORTZEL: Commissioner Slane.

COMMISSIONER SLANE: What concerns me is that as the Chinese build up their nuclear forces, we're forced to cut our defense budget because of our declining economy, and I'm wondering your reaction to whether we will have the resources to counter this build-up, and how you think this will play out?

DR. SCHNEIDER: Well, as I said earlier, I think the military balance is going to shift in their favor over the next decade.

COMMISSIONER SLANE: I'm sorry. Shifted--

DR. SCHNEIDER: Shifted in the Chinese favor.

COMMISSIONER SLANE: Favor.

DR. SCHNEIDER: I mean the cuts of--I mean it's not one--it's not this year's cuts. It's really 20 years of military cuts. You take a look at the big picture and how many advanced U.S. weapon systems of all types have been terminated or delayed or replaced by some inferior, you know, substitute, it really is I think a dangerous situation, and one of the more disturbing things in the--I mean there was very little issue in terms of dollar-wise, but in the current budget that was submitted, the advanced air-to-air missile was zero, and that I think has more impact than a lot of other things with much bigger price tags on it in terms of how the air-to-air balance is going to be shifting.

I mean when the F-22 production was terminated at 187 airplanes, Secretary of Defense said by the time China gets its first--he didn't say J-20, but that's what he's talking about, we'll have 1,700 fighters. Well, we're not going to have 1,700 fighters, stealth fighters, fifth generation fighters. We may have 400 or 450 or maybe even less than 400, and a couple hundred of them are going to be operational.

So when you put all these things together and you take a look at what's happened to the Navy programs with the CG(X) and DG-1000, you know, being terminated or cut back, or in the case of the destroyer to three ships, we're going to have a lot less naval air defense capability than we assumed we were going to have five years ago.

And all of these things have military significance, and I'm concerned about the overall trends that are in play, and I'm not sure we've seen the last defense cuts.

DR. SAUNDERS: If I can just speak to that briefly, I mean I think there are limits on how high China is going to go. As I suggested, I think this is an interactive strategic game. So they are building up their force. Our issue is how we modernize our current nuclear forces and whether we're going to stick with the triad and modernize all three of the legs, or we're going to build new ICBMs, new SLBMs, and think about whether or not we need a nuclear capable bomber.

One way--I think we will fund those programs, but one of the ways you can think about it is do you need to replace them, the capability, one for one if we're in a mode of trying to negotiate reductions with the Russians?

So that's I think part of it, but I think that's a capability any administration is going to keep enough of a secure, survivable and reliable nuclear force. I just think that's a commitment that they're going to make. I think where it gets harder is on the conventional side because there the

capabilities to go operate in or near an anti-access area denial envelope where they're playing at home and we're playing away, that gets a lot harder and a lot more complicated.

You can go at it with high-tech solutions, which stealth was our answer in the 1980s and '90s, to have a high-tech expensive system that could operate in Russian air defenses, that's where you're really talking R&D costs and a lot of expense to build conventional assets that can go operate in that kind of an environment.

That's where it's going to be a lot more expensive, and I think that's where the budget cuts will have more impact.

DR. SCHNEIDER: Could I add one thing to what I just said, please? Certainly, the issue is modernization and sustainment. Right now we're doing a lot more sustainment than modernization. We're not going to see any improvement at all in our strategic force capabilities until about 2030, where whatever the Chinese do--and again, I have no crystal ball--but you're certainly going to see improvement, significant improvements, in Chinese strategic forces a lot sooner than 2030.

So the way I see it, you've got to look at the nuclear part of this in the context of their overall military program, and you know it's probably reached the stage where they're at 25, 30 percent of our defense spending, and they have vastly cheaper manpower, and that's a very disturbing trend.

HEARING CO-CHAIR WORTZEL: Thank you.

Commissioner Shea, or Chairman Shea. I'm sorry.

CHAIRMAN SHEA: That's okay. You've talked about Taiwan as a flashpoint. What about China-India? What is China's nuclear posture towards India, and do they have different strategies with respect to potential conflict with India?

DR. SCHNEIDER: Well, Chinese nuclear capability is vastly greater than current Indian capability, I mean across the board. The quality and the range and the types of warheads they have on the Chinese nuclear missiles dwarfs anything the Indians are doing.

If anything, the Indians have been fairly restrained in the growth of their nuclear ability although they apparently are second--you know, thinking that over again because--they are trying to improve their capabilities to China. They're doing either a very long-range IRBM or a limited range. They have ICBMs now, full coverage of China. They have a program for a submarine with a short-range SLBM, which would be nuclear, on it. So the Indians are doing anything.

The Chinese have, I think, tremendous inherent capability right now to target India, and that will only improve as they introduce the new systems in larger numbers, and if they go ahead with MIRVing the way there are a lot of Asian press reports. That will I think further increase the disparity between India

and Chinese capabilities.

DR. SAUNDERS: The Chinese haven't been so focused on India. They do have units that by virtue of geography and the range of the missiles they operate seem to be about India, but it hasn't been a main driver of their force structure.

I think the concern is that there are tensions that we see from time to time between China and India, and fanned by nationalists on both sides, that make the possibility of a conflict there seem a lot higher than it once was, and I think the other concern is if you think about it as a proliferation chain, Pakistan is engaged in a pretty serious effort to build up its nuclear capabilities.

India thinks about that with respect to Pakistan. India is connected to China. China is connected to us, and how those dynamics might work, right now India has not responded to the Pakistan build-up with an equivalent one of its own, but if it were to do so, then that might make it more of a factor in the Chinese calculus, and so there might be more of a connection there.

CHAIRMAN SHEA: Thank you.

HEARING CO-CHAIR FIEDLER: Thank you very much, gentlemen. That's our final panel for today. I want to thank you for your testimony. I want to thank the staff of the Hylton Performing Arts Center for all the good work they've done to make this possible, and I'd like to thank especially General Cartwright and Congressman Wolf for attending today, as well as the staff of the Commission that put this hearing together.

Thank you very much. We're adjourned.

[Whereupon, at 3:15 p.m., the hearing was adjourned.]

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF MARK STOKES
EXECUTIVE DIRECTOR, PROJECT 2049 INSTITUTE

Prepared Statement of
Mark A. Stokes*
Executive Director
Project 2049 Institute
Before
The U.S.-China Economic and Security Review Commission

Hearing on *Developments in China's Cyber and Nuclear Capabilities*
Monday, March 26, 2012

* *Written testimony only.*

Hylton Performing Arts Center
George Mason University Prince William Campus
10960 George Mason Circle, Manassas, VA 20109

China's Nuclear Warhead Inventory: Alternative Approaches for Research and Analysis

As the United States and Russia continue a concerted effort to reduce the role and importance of nuclear weapons, the People's Republic of China (PRC) remains the only original nuclear weapon state that is increasing its arsenal. While estimates vary, the Chinese People's Liberation Army (PLA) may be expected to double the number of warheads available for deployment on missiles that could target the United States by the mid-2020s. China's declared policy is maintenance of a minimal deterrent and a no-first-use pledge. Ambiguity surrounds how PLA planners define minimum deterrence, and the current and future scope of its nuclear warhead inventory. A general consensus holds that China is increasing its arsenal, including development and deployment of new nuclear-capable delivery vehicles. Yet questions remain as to the extent and intent of China's nuclear force modernization.

In 2006 testimony before the Senate Armed Services Committee, the Director, Defense Intelligence Agency (DIA) assessed that "the number of deployed Chinese nuclear-armed theater and strategic systems will increase in the next several years" and that China currently has more than 100 nuclear warheads. DIA assessed that China likely has fewer than 50 intercontinental ballistic missiles (ICBMs) that could strike the U.S., but that figure could double by 2025. Based on fissile material and delivery vehicle estimates, the Federation of American Scientists (FAS) assesses that China has around 240 nuclear warheads for delivery on approximately 180 missiles and aircraft. FAS also estimates that as many as 140 of the operational missiles are land-based and that 50 of those can reach the continental United States. The estimate of 240 warheads also includes devices supporting the PLA's future ballistic missile submarine force, weapons for bombers, and some for spares.

While these estimates appear reasonable, the potential for a margin of error exists, particularly with regard to future inventory. How many nuclear weapons does China have? How many warheads does China need? If we do not know with a high degree of confidence, what metrics or counting rules could produce the most accurate estimate? An assessment of China's nuke inventory could include four different approaches: 1) strategic requirements; 2) delivery vehicles; 3) production capacity; and 4) storage and handling capacity.

Strategic Requirements

If one placed him or herself in the position of a nuclear force strategic planner, how would one develop requirements? Which specific organization is responsible for developing nuclear weapons requirements? To begin, an initial assumption should be established regarding whether or not a single staff organization develops requirements. While not confirmed, the Second Artillery may serve as the central authority for planning, programming, budgeting, storage, and handling of all nuclear weapons, including those that could be delivered from Air Force aircraft and Navy nuclear submarines. A preliminary review of PLA General Staff Department (GSD) organization does not reveal a nuclear-

related bureau. Drivers and methodology that Second Artillery force planners adopt in developing strategic and technical requirements remain unknown.

More specifically, a tentative judgment is that the Second Artillery Equipment Department is responsible for nuclear force structure planning, with the Central Military Commission (CMC) and Central Committee Political Bureau (Politburo) having approval authority. Nuclear warhead inventory requirements may be developed by the Equipment Department's General Planning Department, with the acquisition carried out by the Special Equipment Management Department. The Second Artillery Equipment Research Academy may play a contributing role. The Second Artillery Headquarters Department Nuclear Security Bureau likely coordinates with nuclear regulatory agencies within China. The Second Artillery Equipment Department presumably oversees research and development (R&D), manufacturing, and follow-on support contracts with the China Academy of Engineering Physics (CAEP). The Second Artillery presumably ensures sufficient fissile material exists to satisfy warhead requirements. Acquisition officers within the Second Artillery likely work closely with the General Armaments Department (GAD) Services Department. Within this department, the Second Artillery and Nuclear Bureau may function as an acquisition policy coordinating body.

Planners may determine how much of a nation's population should be placed at risk in order to deter an opposing leadership from taking action viewed as contrary to Beijing's interests. For example, the Second Artillery may believe that holding at risk 5-10% of the population of other nuclear powers in urban areas, such as Los Angeles, New York, Chicago, and Houston, is sufficient to undercut the deterrent or coercive value of that country's nuclear force. Estimates may be made regarding attrition, or numbers of payloads expected to reach their targets due to losses on the ground or inception in flight. Planning for use of nuclear weapons to support warfighting could increase requirements significantly. However, increasingly accurate and lethal conventional payloads able to achieve the desired effects may dampen incentives for fielding a large arsenal of tactical nuclear weapons.

Delivery Vehicles

The size of China's current and future nuclear warhead inventory likely would be related available means of delivery. Major agreements to limit or reduce offensive nuclear arms that were negotiated by the two superpowers during and immediately after the Cold War focused on delivery vehicles and launchers. Warhead estimates appeared to be based on "counting rules" that credit numbers of deployed warheads to a particular delivery vehicle. In its most recent report to Congress on PRC military power, the U.S. Department of Defense (DoD) appears to assume one nuclear-capable ballistic missile per launcher. The DoD report assesses the PLA has 50-75 intercontinental ballistic missiles (ICBMs), with ranges between 5,400 and 13,000 kilometers (kms), and equal number of launchers in its inventory; between 5 and 20 intermediate range ballistic missiles (IRBMs) with ranges between 3000-5400 kms on an equal number of launchers; and 75-100 medium range ballistic missiles (MRBMs) – presumably DF-21 variants -- with ranges above 1750 kms on an equal number of launchers. In all, between 130 and 195 ballistic missiles are assessed to be capable of delivering nuclear warheads.

Preliminary analysis indicates that China's holds at least 207 warheads in its inventory, assuming one missile per launcher and one launcher per company. The principle discrepancy in DoD reporting could be DF-21 numbers, but this is unclear. Regardless, based on structure and certain assumptions regarding table of organization and equipment alone, China's nuclear warhead inventory could be judged as no less than 200. This figure is based on a notional assessment of Second Artillery order of battle, including at least two DF-5 ICBM brigades capable of reaching targets in continental U.S.; one or two DF-4 IRBM brigades; at least three DF-31 brigades (at least one DF-31A, at least one DF-31, and one unknown DF-31 variant); 10 DF-21 MRBM/IRBM brigades; and one DF-3 brigade. This minimal figure does not include potential tactical warheads allocated to the six short range ballistic missile (SRBM) brigades under 52 Base, the corps-level Second Artillery organization opposite Taiwan, or at least two land attack cruise missile (LACM) brigades. The 200-warhead figure also does not include warheads developed for China's nuclear submarines to be equipped with the JL-2 missile; or possible air-delivered nuclear munitions.

In developing a minimal figure, the premise is that the Second Artillery basic missile launch unit is the brigade, with each brigade having six launch battalions with two companies each (e.g., a "6/2" structure). Each company likely has a launch platform (either silo or mobile launcher) and associated support vehicles in its table of organization and equipment, and stores the equipment in battalion garrison facilities. Therefore, each brigade's table of organization and equipment s assigned at least 12 launch platforms. Other battalions within a brigade are responsible for missile diagnostics, check out, warhead mating, and other functions, usually in an underground facility (referred to as a "central depot") operated by the brigade's site management battalion. As many as six subordinate companies under a site management battalion oversee missile-related preparation, pre-surveyed launch sites, storage, and other facilities. Among site management battalion responsibilities include underground facility management such as power and electricity, water, air conditioning, and ventilation. A service battalion is responsible for security and concealment, camouflage, and deception.

A complicating factor in assessing warhead numbers is that the Second Artillery Equipment Department does not appear to assign nuclear warheads, and perhaps even missiles, to a missile brigade's permanent table of organization and equipment. A central warhead base (known as "22 Base" in Taibai County, Shaanxi Province) and storage regiments under each of the six missile bases (referred to as "Equipment Inspection" regiments) likely maintain custody of warheads, and possibly missiles, during peacetime. Warheads and missiles may be dispatched to site management battalions that are subordinate to missile brigades for assembly in underground facilities for training and during periods of elevated readiness. As a result, the system is heavily dependent upon transportation regiments, reporting directly to missile base headquarters. This hypothesis regarding the relationship between brigades and regiments requires more research. Under this system, the PLA could have few or no "operationally deployed strategic nuclear weapons," which are defined as warheads that are loaded on delivery vehicles and ready for launch.

Production Capacity

The infrastructure supporting nuclear weapon R&D and production also likely shapes inventory size. Assessments of China's nuclear warhead inventory often are based upon estimates of plutonium production and reserves. In 2009 testimony, DIA assessed that "China likely has produced enough weapon-grade fissile material to meet its needs for the immediate future." The International Panel on Fissile Materials estimates that China's two production facilities at Jiuquan and Guangyuan have produced about 20 tons of highly enriched uranium and two tons of weapon-grade plutonium. Assessments of current and future warhead inventory are founded upon estimated amount of plutonium or highly enriched uranium (HEU) needed for a warhead. Assessments of China's fissile material stockpile appear credible. However, research to date should be augmented by a more detailed understanding of China's nuclear weapon R&D and production infrastructure, specifically CAEP. Also useful would be details regarding storage and handling of weapon-grade fissile material. For example, which specific organization – PLA or civilian – is responsible for storage and handling of military-use fissile material?

Storage and Handling

China's capacity for warhead storage and handling also may shape the size of the country's nuclear weapon stockpile. With stockpile security appearing to be of equal or greater importance to operational efficiency and effectiveness, China's warhead storage and handling system is centralized. However, it appears designed to survive a first strike and retain sufficient operational capability for retaliation. Expansion of underground facilities directly supporting handling and storage of nuclear weapons, components, and fissile material could indicate an increase in warhead inventory. While underground facilities could be an indicator, greater precision is warranted. Reliable sources report that the Second Artillery centrally stores most of the country's nuclear warheads in Taibai County, deep in the Qinling Mountains of Shaanxi Province. Base 22 was established under the PLA's Commission of Science, Technology, and Industry for National Defense (COSTIND) in the mid-1960s adjacent to the original manufacturing base in Qinghai Province. Within a few years, the base was relocated to Taibai County in the Qinling Mountains west of Xian and eventually subordinated to the Second Artillery in 1979.

Working closely with the central storage complex in Taibai, each missile base manages a smaller nuclear warhead and missile storage depot. According to an internal Second Artillery account, the depot under each of the six corps-level missile bases store a minimal number of nuclear warheads at any one time. Depots under each of the Second Artillery's six missile bases are referred to as Equipment Inspection regiments. Each regiment oversees at least three battalion-level facilities (literally "equipment inspection sites") with each having as many as seven subordinate facilities (e.g., 21 possible storage sites per base). Missiles appear to be stored separately from warheads.

Conclusion

In summary, uncertainty surrounds China's current and future inventory of nuclear warheads. While existing estimates appear reasonable, the potential for a margin of error exists. At least one approach to validating existing estimates is to examine perceived strategic requirements; operational infrastructure, and current/future nuclear-capable delivery vehicle inventory; industrial R&D and manufacturing infrastructure; and warhead and fissile material storage and handling capacity. Planning assumptions regarding warheads, delivery vehicles, and launch vehicles/platforms remain unknown. A minimal inventory estimate could assume one warhead per missile, one nuclear-capable missile per launch platform (mobile launcher or silo), and two launch platforms per company (two companies per battalion and six battalions under each launch brigade). Based on these assumptions, a preliminary minimal estimate of China's existing inventory is 240 warheads. Additional missiles and warheads available for each mobile launcher could expand this figure. However, beyond assessments of China's fissile material stockpile, another limiting factor could be China's stress on security, as exemplified by its centralized approach to warhead storage and handling, over operational efficiency and effectiveness.