THE BROOKINGS INSTITUTION

CYBER POLICY IN CHINA

Washington, D.C.

Tuesday, December 9, 2014

PARTICIPANTS:

Featured Speaker:

GREG AUSTIN
Professional Fellow
EastWest Institute

Moderator:

JONATHAN POLLACK
Senior Fellow, John L. Thornton China Center
The Brookings Institution

Panelists:

KENNETH LIEBERTHAL
Senior Fellow, John L. Thornton China Center
The Brookings Institution

JAMES MULVENON
Vice President
Defense Group, Inc.

* * * * *

P R O C E E D I N G S

MR. POLLACK: Good afternoon, everyone. We much appreciate you coming out on a rainy afternoon for what I think will be a most interesting event.

I'm Jonathan Pollack, senior fellow in the John L. Thornton China Center, and we're very, very pleased to be able to host this book event here today. Few policy issues related to China have generated more headlines and more controversy in recent years than the question of China's interest and shall we say, its involvement in cyber technology and information technologies more generally.

We are really privileged today to have Greg Austin as our speaker. Greg is a professor -- what do they call you, Greg? You're a professorial fellow at the EastWest Institute, which for those of you who are not familiar with it, it's headquartered in New York but has offices, I believe, in Europe as well.

I would say parenthetically about Greg Austin, that it seems to me every 10 years Greg has another book that is ahead of its time. In the 1990s, he wrote a book about China's pacific frontiers, well before anyone talked about major questions related to the maritime environment in the East China Sea or South China Sea, and I still commend it to you; it's still hugely relevant and I recommend it. He then did a co-author book about 10 years after that, I guess, on China and Japan, which prefigures, I think, a lot of the controversies that we see. And now he has yet again waded into controversial waters with respect to his new book on cyber policy in China.

Now, I want to give Greg a full chance to present his arguments. These are arguments, both about China's pursuit of information technology, but putting it in a much larger political, social, and economic context, not just simply grabbing at the headlines that we often see devoted to this topic.

At the same time, we are very, very fortunate today to have two truly

outstanding commentators on Greg's book. First, my good friend and colleague, Ken Lieberthal, and then someone that I knew from when he was a mere graduate student at UCLA many, many years ago, and actually someone who collaborated with me on some important work years ago, and this is James Mulvenon, who is the vice president of Defense Group, Inc., where he also heads their group on the Center for Intelligence, Research, and Analysis. I may not have named -- did I name it correctly? Something -- yeah, CIRA. Yeah.

Anyhow. But I should say that both Ken and James have worked in great depth on issues related to cyber policy in China. James does all kinds of work for the U.S. Government on these issues, and to the degree possible, tries to be able to make his views known in contexts such as this. So we're pleased to have him here today.

Ken is well collaborated with a former colleague of ours here at Brookings on questions of cyber in China, some of the policy issues that are raised. So I think we're going to have a very, very healthy discussion today. But we'll begin first with Greg, who will present some of the core arguments in his book.

Greg, welcome to Brookings. We're delighted to have you here and really look forward to your remarks and the discussion to follow.

MR. AUSTIN: Good afternoon, ladies and gentlemen. Thank you for coming out, as Jonathan said, on this rainy and cold day. I've come two weeks ago from Australia, where it's very different.

Let me just say first thank you to Jonathan, Ken, and James for setting this up, and for Ron McIlvaine in the China Center. It's a very great opportunity to be here to present to our Washington audience and a Brookings audience.

I'm going to make a presentation today around the book, but I've titled

the presentation somewhat differently called "China's Race for Cyber-Enabled Power." So I just kept to that term -- cyber-enabled power. And I'm using that term partly because we don't have a good word yet to describe the cyber environment or the information society environment which captures all aspects of it. So almost any word you pick to title a book is not that good.

The second point I'd like to raise about that title, cyber-enabled power, is that we can see it in much the same light as John Hay term, soft power. Now, I don't claim to be anything near the status of John Hay as a scholar, but he coined this wonderful term "soft power," which described a certain set of activities, and in a sense a changed set of international circumstances. So I think it's quite legitimate to think about cyber-enabled power as a changed set of circumstances and a particular set of activities.

Before I launch into my remarks, I'd just like to acknowledge General Henry Raddick, who has been a long-time supporter of the EastWest Institute. We've been working for about five years now on cyber power issues with the United States-China teams, with the United States-Russia teams, and (inaudible @) on cyberspace cooperation. Harry is a senior counselor with the Cohen Group, and a senior advisor and head of the Risk Advisory Services Group in Deloitte. So thank you, Harry, and good to see you.

Our presentation will have three parts basically. The first part sets the global context. The second part looks at China's leadership values in addressing that global context, and then there will be a third, very brief section, which is the conclusion. Jonathan has full authority to call time-out on me when I hit 25 minutes, so I'm going to try to catch a very dense set of materials and ideas in that 25 minutes.

In giving today some rather critical analysis of China's lack of achievement in its ambitions to become an advanced cyber power, I want to first take off

the proposition that China has, of course, made significant advances in the field of information technology and in the application and understanding its application in society and in global politics.

I'll just take off five very quickly.

China's Lenovo is now the biggest PC manufacturer in the world. China has more "netizens" than any other country. In the advanced science of information technology, Chinas scientists reported in 2012, the first teleportation of quantum information between remote particles. We can discuss later what that means. But what it means is that there are Chinese scientists working at the frontier of quantum computing, which is judged by many specialists around the world to be not only very important in a range of civil applications, but very fundamentally important in a range of military applications.

China is also taking a lead role in engineering and the Internet Protocol Version 6, and China has a clear position amongst the world leaders in building the fastest super computers. China has also, as we know, built the largest surveillance system in human history in terms of manpower and the degree to which it's cyber-enabled. We also know that China is very good at cyber espionage.

But there's a conundrum here. In the last four years, since 2011, the World Economic Forum, which every year reviews a global system of rankings of each country in terms of its network power or network readiness, in that index system of rankings, China has slipped from its 2011 position of 36th to its position in 2014 of 62nd. But here is this rather prestigious global index saying that China, which is vigorously pursuing all aspects of cyber power has, relative to the rest of the world, since 2011, slipped from a ranking of 36th to a ranking of 62nd.

Now, there are all sorts of weaknesses in that index. One of the biggest

is that it actually has a number of sub-index elements which are per capita based. So, of course, China was disadvantaged in that per capital situation. But there are other indexes around which reflect a similar sort of opinion, and just recently, the Shanghai Academy of Social Sciences published a list of the 20 smartest -- or did a survey of 20 smart cities in the world. And they're not the top 20. It had to find a way of getting two Chinese cities into the 20, so it picked 20 big cities that we all know about.

And what's interesting is that in that list, China's two big cities in the list, which are Shanghai and Beijing in that order, sit at the end of the list between Moscow and Mumbai. So that's one way of saying that China sits between the Second World and Third World in terms of cyber power. So we're in a situation really where the Chinese leaders are confronted with assessments from their own specialists; that China is actually still lagging behind in cyber power and it's slipping off the pace.

One of the key reference points that I picked up in writing this book was very different from what I thought I would finish with when I started. I thought I'd write a book about China's cyber frontier, like I'd written a book about China's ocean frontier, but I found that the reference points for the Chinese leaders were very different. They had this idea of advanced information society. They'd embraced this very fully around about the year 2000. They were not the first to do it, and they were about 20 to 30 years behind the play compared with other countries in adopting it. It was part of a global movement in 2002-2003. The United Nations system convened something called the World Summit on Information Society, which recognized at global level and with all states participating, this transformational effect of advanced information technology and its applications in society and the military sphere.

To write the book and to try and come to terms with this massive information and massive, very disturbing headlines about China's cyber policies, I wanted

to find an analytical structure. So the analytical structure I settled on was trying to understand what were, say, the top nine or 10 values that the Chinese leaders would have to have it they wanted to pursue an advanced information society.

So I came up with nine ideal values for what I call cyber-enabled power or an information society. There could be 12. In fact, I started with 12 but 12 was too many for the book, so I came back to nine. They're in three buckets.

One is the national information ecosystem. What goes with this idea of an information society and a chain set of circumstances, a transformational set of circumstances, is that one of the most powerful determinants on any country's policy is the information ecosystem in which they live. There's a national component to that and an international component to that. Some would say it's just one ecosystem without any boundary.

So under the national information ecosystem there are three important principles -- freedom of information exchange, protection of information exchange, and trusted information.

The third bucket concerns the innovative information economy. If you want to become an advanced information society, the leaders have to have that transformation intent. They have to be determined to change the country and determined to change the economy and to make all of the structural adjustments and changes that go with that. As well, the country has to have an innovation system and a class of innovators. I'll return to those later.

Returning to the global information ecosystem, which complements the national information ecosystem, there are three things which governments really need to become an advanced information society. This flows from the proposition that advanced technology is fully globalized, highly internationalized, and doesn't fit in one country.

So the three things that you need if you want to be an advanced information society -- strategic stability. You have to be out of bridge military divides, and you look ultimately towards help from other countries to solve your problems, what the Chinese call interdependent, informatized security. So you'll see later that this idea of interdependent, informatized security is something which doesn't get much pressure at the moment in terms of where China sits globally.

So jumping quickly to the second part, where does China sit? And I just want to give a very rough idea of a timeline here. So through the Cultural Revolution, and really up to about 1980, you could describe China, if you wanted to oversimplify, as a scientific black hole. Prior to China in 1980, as a country with households of light bulbs, where in the majority of households in China the only electrical apparatus was a light bulb. So in big picture terms here, China was mostly a rural economy. I've heard a Chinese PLA officer make exactly this observation. It wasn't original to him or me; it came from a German scientist in 1983, who made a visit to Hong Kong when I was there.

In 1993, Chinese leaders had made a very clear commitment to becoming an advanced information economy. So they thought that if they built all the computers that they wanted to and that they could, if they had an advanced electronics industry, they would be able to do what the rest of the world did in terms of information economy.

The Internet came to China in 1995, but by the year 2000, at the same time as the rest of the world was adopting this idea of a world information society and national information society, China moved decisively in that direction itself, and the leaders clearly plumped for a strategy to build an information society in China. That had immense political implications, which have been well studied by authors of more than 20 very good books on the subject. But that was a decision they took in 2000. And just like

the decision to admit the Internet to China was a risky one, so, too, was this decision in 2000. It carried inherent fundamental challenges to the long-term plan.

By the year 2014, President Xi declared that China was falling so far behind in its ambitious to become an advanced cyber power that he personally would take control of the leadership group responsible for it and he said he would do everything it took, and the Chinese Communist Party would do everything it needed to make China an advanced cyber power.

So how is it that after 30 years of ambition, struggle, and great achievement with quite a few setbacks, but basically with great achievement and great forward momentum, how is it that China ends up slipping from 36th to 62nd over the last four years in the global system? Well, it's because China's leaders don't really follow those nine values that I identified as central to becoming an advanced information society.

So if we just go to the national information ecosystem -- and I'll pass fairly quickly over this -- when it comes to freedom of information exchanged, which is absolutely central by its nature to the whole idea of an advanced information society, we know that the Chinese leaders prefer the situation which I've called I-dictatorship, or information dictatorship.

When it comes to protection of information exchanged, we know that the Chinese leaders prefer recourse to laws on state secrets rather than let basic scientific data throughout the society and the environment circulate.

And in terms of trusted information, the info sphere and the Internet environment in China is anything but trusted. There are threats from all sorts of sources -- criminals, as well as the government. But you can't really trust the information on the Internet, and surveys among Chinese netizens show a much higher mistrust of the

Internet than you see in other countries in the West.

So in that very important area of the national information ecosystem, the Chinese government is still not doing what they need to to make the right leap into advanced IT science, into advanced science, because they close everything off -- they shut it down. That's changing, of course, but that's still the basic, overriding policy center -- policy setting.

I'll just make a little bit more detail or comment on the innovative information economy because that gets a little bit less press, and then I'll pass to the question of the international diplomatic environment -- international ecosphere.

The first of the three values I mentioned as important under the heading of Innovative Economy relates to transformation intent. Are these Chinese leaders fully committed to transforming their economy into an advanced information economy? Well, interesting, the answer to that is yes. And they have a very hard rhetorical equipment, and China ranks in the sub-index, or the relevant sub-index of the World Economic Forums Global Index. China ranks above all other J-28 countries and the commitment of its government to becoming an advanced information economy and an advanced information society.

So there's a big gap between leadership intent in terms of innovative economy and performance. And if you look at the penetration of advanced IT in case sectors, like manufacturing education and agriculture, the pace has been really very slow. And that's not my assessment; that's the assessment of China's professionals and it's the assessment of a lot of international economists who have worked on it.

As a footnote, beginning in 1999, the State Counsel of china has worked very closely with the World Bank and published a report at, I think by now, four different phrases of their informatization program. So the World Bank has been a key adviser in

China's efforts to become an advanced information society.

The one area where informatization has penetrated rather significantly in China is in the case of public health. And one reason for this is because of the size epidemic. And the size epidemic in 2002-2003, exposed the Chinese position on censorship or information about basic public health, public safety, and public interests activities. And so the health system is being transformed somewhat, in a way relative to other sectors, which has benefitted from that negative experience of the SARS epidemic.

When it comes to the second value that you need to build an advanced information society, the idea that you need a national innovation system, how has China fared?

Well, China has made some really top and tough political decisions on this point. It decided in 2005, that it could not become an advanced innovative society if it did not let the private sector lead innovation. This is very anti-communist party. It's very out of character for the Chinese Communist Party to admit that it can't lead the national innovation strategy of the country; it has to be private sector led.

And in that process, probably for the last 30 years as much, China has relied heavily on the Chinese Academy of Sciences, which remains a really powerful, and I think very productive organization, very impressive in many ways. But it hasn't been able to translate -- the Chinese government has not been able to translate into practical outcomes, the investments that it needs from the private sector into the universities and even into the Chinese Academy of Sciences. And the very year after, the Chinese government said that we need the private sector to lead innovation. The statistics on private investment in R&D were very bad and the statistics on government investment in R&D were very high. So there had been an increase. So there are quite a few contradictions that we need to look at.

Interestingly, in the World Bank Report jointly authored with the Chinese government called China 2030, which was not exclusively about information technology but about China's overall national development, was the hardest hitting World Bank Report published over this sort of 10 or 12 years in which it was involved with the Chinese government. And you can see the 2001 report, which wasn't published really in full, and in later reports, the World Bank has gone quite soft on the Chinese, but at the time they got to China 2030, they basically said, China, you just don't have it. You don't have most of the policy settings you need if you want to become an advanced information economy. And there's a nice little quote, which I've pulled out, which helps illustrate that. They said, "Innovation of the technology frontier is quite different in nature from simply catching up technologically." And there is where more or less the World Bank said China had settled.

The third element for an innovative information economy that I mentioned is that you need to have an innovative class. I won't dwell on this. Perhaps we can return to it in question and answer in the discussion. But by and large, China has made outstanding efforts since the year 2000 to expand its tertiary sector, especially in information technology. The expansion in information technology studies in China after 2000 is massive. It's probably one of the biggest expansions of tertiary education seen by most countries for a long time.

But China does suffer from a brain drain. The latest statistics I've got from a Chinese source are that something like 40 percent of Chinese students sent overseas to study return and the government regards that as very low. But the figure for the United States, which I have, which is not entirely reliable and could be challenged, is that the figure for returnees from studying in the United States is about 25 percent. So the best and bright from China are not going home.

This is accompanied with the crisis in universities, which I understand to be oriented largely towards the desire of the Chinese communist party to keep control over the universities. Promotions at Chinese universities are still very heavily influenced by your relationship to the Communist Party, and in fact, whether you're an active member in it. But there are other considerations which people I've met cite as the reason why they didn't want to go back to China after studying in the West, and they relate to the social environment. Things like "one child policy," freedom of conscience, and the ability of "labor and freedom." So China is not doing well in terms of building that innovative class that it wants.

Looking ahead towards the future for China, I think China will have to address some problems of venture financing and will have to become more open to foreign partnerships than it is now and foreign penetration than it is now And I think those two things will happen. There will be political conflicts around both those things but I think those two things will happen.

Let me just finish off this section of the presentation with a quick reference to the three ideal values for the international system, the global information sphere. I mentioned strategic stability and I mentioned that countries should pursue a situation where they can overcome military divides. And a country should aim for interdependent, informatized security.

Before addressing those three points quickly, I just want to give you a timeline of PLA development in the cyber sphere just as a quick reference point to parallel what we heard on the other front. In 2001 or thereabouts, the PLA joined the leading group on informatization. In 2002, 2003, or thereabouts, the Central Military Commission made a decision at doctrinal level to shift towards war under conditions of informatization. It proposed two stages, 2020 and 2050. In 2006, it approved training

regulations. In 2011, it made changes in the general staff department communications structure, and then in 2014, as I mentioned, Xi Jinping took over, basically saying, "You're not doing a very good job, guys."

So strategic stability. How has China done? China has a strong commitment in principle to a stable world order. It does want an adjustment of the balance of power more in its favor. It is committed to position the country for long-term cyber military power, but it is concerned also about the United States' capability for preemption in military operations. And this concern extends to strategic nuclear weapons. We can discuss that later.

As much as China may want a peaceful and stable world order, it sees itself as somehow tied up in a global cyber arms race. It is an aggressive actor in cyber espionage, and there is a clear conflict between some of these different aspects of how China regards strategic stability. But looking forward, we can ask the question whether or not China will work to resolve those.

How am I doing for time? Okay.

On the second point, the second point about bridging divides, the idea here is that if you want to become an advance information society, you've got to be able to access all of the investment, all of the technology that other people have that you don't have and that you judge that you need. Well, in this particular undertaking, it just so happens that Taiwan was one of the leading sources of technology and investment in this sector, and one of China's greatest achievements in the last 20 years in terms of becoming an advanced information society is the way it has developed its relationship with Taiwan. By 2010, 2012, or so, China had replaced the United States as Taiwan's main economic partner, and China was a significant investor, as was the United States, in China's ICT sector.

So the payoffs for China in pursuing this policy of bridging divides has been very spectacular. At the same time -- and we can discuss it later -- it's adversarial view of the United States has deepened and we see how that adversarial view, both in China and here, has had a very negative impact on the deeper integration of the ICT sectors of the two countries, Huawei being a case in point.

The third value I mentioned, which is very important for countries wanting access to this investment in technology and to become an advanced information society operating in a globalized world is a commitment in principle and practice to cooperative norms and economic and technological aspects of the global information economy. And the strength and commitment to joint problem solving in nonmilitary domains. And China is working in these areas. It really gets very little attention. China is committed in principle to cooperative norms and economic and technological aspects of the global information economy. But we have to admit also that China has been unable so far to bridge its formidable differences with the United States and like-minded countries over Internet governance and network security.

So looking ahead on the international front, where might we end up? I think the timetable of 2050 for full informatization of the armed forces should be attainable. There will be considerably more successes in cyber espionage, but so, too, will China's adversaries have such successes. But I see no prospect that China will make any appreciable dent in the information superiority of the U.S. global alliance system. That has some consequences.

At the same time, I do think that China's race for capability in this field will take more account of diplomatic costs, such as those that are occurring in the United States and Europe because China needs a globalized economy more than it needs the cyber espionage and the destabilizing activities that it's undertaking. And I predict that in

the short-term we'll see -- okay.

So here we go. Conclusions. Very short.

The main conclusions in the book that, as I've suggested, China's censorship policies and its closed education system have contained its ambitions to become an advanced technology country. China's leaders are deeply concerned about the difficulty of building a high-performing national innovation system. They are deeply concerned about the difficulty they face in building a high-performing national innovation system. They've tried almost everything they can over about 15 years and they're just not getting what they need. China has proven itself incapable of resisting the powerful transformation effects of the information age. We can debate that a little more what that might mean in detail.

Apart from the conclusions in the book, I've just got three quick points which I'd like to mention about what we can learn from this overall picture. I think we can learn that China and the United States are both subject to an information revolution that is transformational and not defined by the policy preferences of either. We also learned that China's cyber-enabled power will remain heavily dependent on private sector actors and governments in the United States, Japan, and the European Union, what I call, and some will see the humor of this, perhaps, or the irony, the greatest lawful transfer of wealth in human history.

The final point that I think I learned from writing this book is that the proposition, which is not original to me, is the idea that knowledge has no flag. And I think if we contemplate the meaning of that and how that plays out in terms of technology transfer, and really, how it informed U.S. policy towards China for decades, then we can end up in a different place form where we are on some of the more topical policy issues.

Let me stop there. I think I've put on the table a few issues. Thank you.

(Applause)

MR. POLLACK: Greg, thank you very, very much. I'm reminded of an observation that I heard at a meeting in Beijing several years ago where what we see with China, it's an analog system that's trying to operate in a digital world. And he's raised so many questions that I think really warrant more extensive discussion. So for now, I'm going to sit down and introduce our two discussants who will explore these issues in greater depth. And then from that we'll have a conversation here on the stage, and then subsequently, we'll open it up to questions from the audience.

So first, Ken Lieberthal.

MR. LIEBERTHAL: Thanks, Jonathan. And thank you, Greg, for a masterful overview of what was a fascinating book. I really liked Greg's framework of analysis for this book. Thinking in terms of what are the essential values for developing a full information society; a society that takes full advantage of the ability to generate, analyze, utilize information for societal transformation, for economic innovation, and for helping to define its role in a global set of problems and a global ecosystem. And Greg did a great job of using just a few minutes to highlight what his basic conclusions are in each of these value areas. I'm not going to try to pick that apart in any way.

Rather, I want to use my few minutes to expand the last if issues on our agenda and really look forward to any comments Greg wants to make about whether this expansion, whether what I'm going to try to add to the agenda affects the way we might think about China's future in this informatized world or informationalized world or whatever you want to call it. The Chinese is easier than the English when you talk about this.

I think the dimensions and dynamics of an information society are on the cusp of qualitative change. Within the next 5 to 15 years, the dynamics of the information

ecology, if you will, will be dramatically different; not just simple straight line extrapolation, but dramatically different, I believe, from what we now confront. This inevitably will be affected by things that no one currently anticipates, but even if you stick with the relatively known things, the things that are already underway and where you can look ahead and contemplate their implications, is really quite dramatic. And I will base my kind of short list of five or so of these items on two sources, although, I mean, it's actually based obviously on a lot more than that.

About a week ago there was a conference that was written up in a number of ways in the media on the seventh U.S.-China Information Forum that several of the people in the audience I know were at, and just issues that were raised there, not so much as what the future looks like in the information world.

Secondly, *The New York Times* over the past week and some of the issues that have come up as news stories in the past week, not focused on China but focused on the information world. My short list of things that are already well underway but are going to change the ecosystem for the way we think about an information society, within five to 15 years -- this is not science fiction 50 years from now -- include the following.

One, the Internet of things. I don't know how many of you have heard of that concept. It is that increasingly things -- the clothes you wear, the gadgets you deal with, the furniture in your house, the car you drive, the street you walk on, you name it -- will be in constant contact wirelessly with the Internet, generating information about its own situation and its immediate environment as pertinent to its own condition and its future needs. This is effectively putting sensors in everything you can imagine and having those sensors communicate wirelessly with the Internet; not based on your instructions to communicate but simply communicating.

We all carry around such sensors now. For those of you who have an iPhone 6, you've got at least 10 of them in your phone that are constantly sending out information regardless of what you're talking about.

I actually -- as I was preparing this, I looked at my iPhone and thought to myself, "Well, I wonder what this is sending out that I don't know about in addition to the things that you do control." And I saw an icon there that comes with the phone. It says "Health." So I clicked on health just to see what it's recording. And it tells me how many steps I take every day, how far I walk every day, what time of day I do that, how many flights of stairs I go up and down. I didn't know it was keeping track. I've never opened this. So I looked on the list of things that I've enabled and I never enabled it. It's just there. And it's not there just for my own information. It's communicating this every day. I went to China and I was actually on a flight for 24 hours. It turns out this registered as basically I had died for 24 hours and I resumed living again.

But anyway, this is producing an explosion in the amount of data digitally being put out onto the Internet. Not for everyone's casual acquisition and use but it is phenomenal. It is a dramatic increase in the kinds of data and stream of data being put out there. And one figure used at the Internet conference last week was that there are now, as I recall, 16 billion, roughly, wireless, you know, devices that communicate wirelessly with the Internet, and that by 2010, there will be 40 billion. And that number will keep growing a great deal.

Secondly, there is a fundamental expansion in the capacity to store data very cheaply. It costs almost nothing to store data now. And so we are all moving our data into cloud computing so that you have these massive data farms that can store almost inconceivable amounts of data. So as the data grows, these data remain available within security walls, but remain available and accessible. And the power of

algorithms to search, assemble, and analyze that data is largely removing the previous truism that if you want to find a needle in the haystack, the worst way to do it is to enlarge the haystack. Now the size of the haystack increasingly is irrelevant. You collect the data and you can then ask questions of that data in new and creative ways, ways never thought about when you collected the data and still very efficiently find answers to those questions.

That relates to the third major development. Some of you may have seen an article about Stephen Hawking this past week in *The New York Times* where he was warning about the advances of artificial intelligence to the point where the software will get ahead of the human controllers of the software because software is, you know, this is an evolutionary process but increasingly is able to put together things in order to learn as it analyzes; to upgrade its capabilities, therefore, as it goes along. And increasingly, even to correct previous errors and learn how to do better without human intervention in the process.

And so the assumption -- one thing that we're always ahead on is at least we can always unplug the computer. Computers are there to follow instructions, and those instructions can be enormously complex and they can do it at enormous speed with enormous brute force and so forth. At the end of the day, that is beginning to shift.

I heard Bill Gates talk about this a little over a decade ago, just at a dinner party, and his concerns that within 20 years or so the power of software would get to the point where it was no longer really full controllable by those who write it and who seek to direct it.

Pete Singer, formerly of the Brookings Institution, wrote a great book called *Wired for War* on the increasing use of drones and robots in various aspects of warfare, and one of the more intriguing parts of the book was looking ahead to the

questions that will arise about what do you do when drones can be used increasingly autonomously? And then how much do you allow them autonomy to do things where they may be able to do it better than if you have a human being in control of them at all time and having to make decisions. And then what are the implications of that in a wide array of ways? So this is an issue that is increasingly on the agenda and it's not sci-fi for 100 years from now. This is something that is emerging in a timespan that all of us normally think about for policy purposes.

Fourth, information security. And I would certainly yield to James on this for a more knowledgeable comment than I can make. But my sense is, and experts I've talked with have generally affirmed this, that information security is actually decreasing rather than increasing. The capacity to defeat security measures is growing more rapidly than the capacity to protect data. Government regulations are almost inevitably way behind the dynamism of innovation, technological innovation from the private sector, from universities, and so forth. Let me say most of those who make up government regulations are older generation, and older generation is not ahead of the curve generally on cyber development.

There's also a potential fundamental game changer that Greg mentioned in his -- one more minute -- that Greg mentioned in his presentation, and that is the development of, at some point in the foreseeable future, likely full development of quantum computing. And that is a game changer for reasons I'll let James or Greg explain the details of, but fundamentally, if you think passwords will protect anything in the age of quantum computing, you must be kidding. And I believe also the same is true of sophisticated encryption. There's just a capability for speed and an array of approaches simultaneously. Quantum computing just changes the game-on completely.

So where you have these vast aggregations of data with sensors feeding

that constantly in one way or another, offense already ahead of defense, quantum computing potentially on the horizon and not the far distant horizon, what kind of world are we into? And what are the issues that that poses? It's not only whether the government controls information but who controls information, who accesses information, who can utilize information. And that is especially true, and I'll end on this, given that there's been a major evolution in the focus of information gathering, which is to say that increasingly information is being gathered centered on the individual because that's how you better anticipate individuals' needs, tastes, wants, problems and so forth, and provides services to meet them.

I don't know about you; I find on my iPhone 6 now when I type a message, more times than not the computer is suggesting the next word or phrase and it happens to be the one that I would use. So it's not just from context; it learns what I like to write, how I like to express myself. And half the time I'm just hitting a button saying, "Yes, use this for the next thing." And then I sit back and say, "Gee, don't I have anything different to say?" And some human control over what information is generated, how it is utilized, who -- human, machine, local, national, where -- accesses it and so forth is changing very rapidly and potentially, fundamentally. My question is how much we should be adapting the top priorities in our own agendas as we look at developments in China and elsewhere in the cyber domain.

Thank you.

(Applause)

MR. POLLACK: Well, I know that apple is getting all these free advertisements, not that it needs it. I just got my iPhone 6 yesterday, so Ken has already enlightened me about all the things I don't know about what this little machine is already doing while I'm not paying attention to it. Sometimes they say "ignorance is bills," but I'm

not sure in this case that it applies.

With that as an introduction, James, please. The floor is yours.

MR. MULVENON: Thank you, Jonathan.

I know I mentioned this the last time I was at Brookings, but the canonical story for me kind of about the Internet of things is that I recently renovated my kitchen, and I monitor my home network fairly carefully because I have two teenage daughters. And I caught my refrigerator trying to communicate out through my home network back to General Electric to get a firmware update. Well, the first problem is I didn't know that my refrigerator had a wireless antenna, and I certainly didn't authorize it to hack out through my home network to try to get back to Mother General Electric, but we're at the forefront of the Internet things.

Well, I actually just closed the high, nonstandard port it was trying to use to get out. So, they knew they were doing something wrong. It did point out that my water filter wasn't working properly.

Thank you to Jonathan. Thank you to Brookings for having me here today. I have to make an early disclaimer, which is that, of course, my comments bear no resemblance to anything advocated by my wise and generous, though sometimes humorless, highly paranoid and mercilessly unforgiving U.S. government masters.

And unlike Ken, I'm going to talk about Greg's book. (Laughter) I'm trying to be very filial. Okay? You know, Ken is my former teacher at Michigan and Jonathan was my former supervisor at RAND.

Unlike most writings that I read in Chinese cyber, including my own, Greg's book is admirably evenhanded and fair. And I think that he reports China's aspirations across a wide variety of areas, that really is the strength of the book, is that it is not just boar-sited down on the intrusion sets or on military cyber warfare writing, but

really talks about informatization in the same incredibly broad gauged way that the Chinese themselves talk about it, which is that it is the use of information and communication technologies in order to facilitate developmental leaps across society, the economy, the political sphere, diplomatically and militarily. We do not really give enough credit to just how incredibly cosmic the concept of informatization is in China and the importance that they subscribe to it as a strategy across all sectors of development.

But Greg takes their aspirations seriously, but he also doesn't flinch from calling out the Chinese government and its various actors when they fall short of their stated aspirations. And so one of the strengths of the book and one of the themes of the book that is implicit and that I would call out more explicitly is this interesting set of dichotomies. On the one hand, the dichotomy of the Chinese government's clear use and the value they see in e-government and using the Internet as a platform for proto democratic articulation of preferences at lower levels and things like that, while on the same side, correctly characterizing their censorship regime as ironfisted, and as Greg said, the biggest and most advanced surveillance apparatus in human history.

Another dichotomy that he brings out is the dichotomy between, on the one hand, the way China is trying to innovate between trying to facilitate private sector innovation but yet seemingly always then leaning back on the old standby which is state centrally planned, driven innovation. And this has certainly been the frustration that they have clearly exhibited since 2005, since the 2006 to 2012 mid to long-range S&T plan was issued, where their go-to, when the private sector fails to deliver something, is to instead put out a large strategy backed by (inaudible) enterprises, large amounts of funding, have large interagency groups involved. And then when that doesn't work, increasingly turning to cyber espionage and other ways of achieving illicit tech transfer that I talked about in my book.

Another interesting dichotomy is the dichotomy that he brings out between on the one hand the strategies that China is pursuing that I just described and how they are remarkably ill-suited from an organizational posture to actually carry them out. And so you have the cheap leather jacketed and sun-glassed thugs from the Ministry of State Security on the one hand, who are trying to push through highly nuanced and sophisticated cryptography policy. It's the wrong guys for the job, really.

The first time I ever met with the State and Christian Management Bureau I knew immediately they were MSS, not because of what they said, not because of where we met, but because of their clothing.

He also points out the dichotomy, which I think is really interesting in China between on the one hand what technology enables and on the other hand how interesting aspects of Chinese military command culture, PRC political culture under single-party rule, the Chinese Communist Party, and even Chinese culture, in fact, sub-optimize the way that that technology can be employed in various scenarios.

And so I agree with him fundamentally that what he describes as "an ethical dead-end, the summation of all of these contradictory policies said, you know, simply pointing out that because of those contradictions that there will be this tension, there will be these failures, there will be this continued inability to reach and achieve those successes.

But the second point that I'd like to make though is to actually explore this dualism itself as Greg calls it. As we used to say at RAND, are these curves converging? Or are China's aspirations and reality converging on one another? Or is there something more fundamental that is structurally preventing them from achieving the things that they explicitly at great length lay out in their documents as what they're trying to achieve? And I will resist cultural exceptionalist tendencies to talk about the greater

capacity of the Chinese mind to hold two contradictory thoughts in their head at the same time or something like that, and instead point to some interesting dichotomies that I think parallel many of the things that Greg has highlighted that continue to trouble me more on the strategic side of things and then come back to the information society.

As I've watched over the last 20 years, China's economic and political and diplomatic and military power grow, I have been struck by two curious lag effects. One is the lag effect in China's ability to do crisis management, which has been in stark relief in '99 with the Belgrade Embassy bombing and in 2001 with the hostage crisis. And also, more importantly, China's inability or sort of tone deafness in terms of strategic communications, really not achieving what they want in terms of the messaging that they do to the outside world. And it really comes down to a dichotomy between the propaganda of the word and the propaganda of the deed. And so we increasingly find ourselves trying to analyze a China that for illegitimate political and ideological reasons continues to hold onto traditional principles, like the Five Principles of Peaceful Coexistence, like the No First Use policy, that are increasingly at variant with what we actually see in the reality on the ground.

So, for instance, the Five Principles of Peaceful Coexistence, one of the key ones is mutual noninterference in the internal affairs of other countries. The problem is ever since the go-out strategy, we see China regularly interfering in the internal affairs of other countries. In fact, one of the perks of being a great power is interfering in the internal affairs of other countries. It sort of comes, you know, it's one of the bennies that comes along with being a great power. And, yet, China continues to insist that it's not doing that because of their moral, self-righteous position of the Five Principles of Peaceful Coexistence. Similarly, we see developments in the modernization of the second artillery, which at some point is going to reach a tipping point in my view where

they will continue as they have said, to continue to say they have a No First Use policy even when the force on the ground may, in fact, be a limited warfighting force to (inaudible).

So as an outsider looking at that, you know, depending on who you are and depending on our own ideological position, you look at the gap between what they're saying and what they're doing and either you ascribe strategic deception to it, and there certainly is a cottage industry here in D.C. for that. Or you ascribe it as I do to largely bureaucratic dysfunction and the inability of key players in the system to actually rise above the stated principle and call out the stated principle because of the way that their political system is structured. And this has big implications. This dichotomy, this sort of multiple messages, this schizophrenia, if you will, has incredible implications for the United States in terms of escalation control, in terms of strategic deterrence, in terms of all manner of the inner actions of our policies. If we are constantly trying to translate what they've said to what they're actually doing and not being able to do it because they don't match, you know, then it becomes the limits of our imagination as to how do we bridge those gaps.

Now, what I was struck by and reminded of when I read Greg's book was the structural problem that I think underlies this sort of main issue about why they are not achieving the marks that they want to achieve. It's that the Chinese government has gone to a lot of meetings and killed a lot of trees and spent an enormous amount of money to try and force concepts like an advanced information society in indigenous innovation without recognizing that both of these things, in fact, require very organic, non-forced, evolutionary sort of ingredients that you cannot be forced through government fiat, that cannot simply be bought with more money, cannot be achieved by trying harder and throwing more people at the problem if they are, in fact, in some cases a very fragile

combination of society trends that come together to allow a society to become an advanced information society. And without being a complete Homer, you don't read the U.S. Government putting together massive national plans and spending billions of dollars and having enormous interagency meetings in order to create an information society in the United States. Why? Because the combination of all of the social and economic and political factors and technological factors in the United States allowed it to organically develop all on its own. And that's the resilience of it. You simply can't force these issues. And yet, the Chinese government believes -- wrongly, I think, when they look at Singapore and other countries -- that that was the secret to their success, which to me is a misunderstanding of Singapore. It's a misunderstanding of all the exemplars that they use.

And so finally, let me close by asking the question how do we -- how are we supposed to then interact with such a schizophrenic actor? I think the key is -- and we don't do enough of this -- is to actually, very carefully read the reams of my numbingly boring material that they put out. And one of the strengths of Greg's book is that he, in fact, catalogues an enormous number of 100-page strategy reports that I would argue that a very small percentage of people who study China have actually read. I'd have to force myself to read those documents by saying, "Come on, James. There's at least one interesting thing in this article." That's what I tell my analysts who are like, "Oh, not another Shinal article." I say, "You find the one interesting thing in it. Okay, there's one interesting thing in every article. It might just be an adverb, but you've got to find the one interesting thing in it. So carefully read what they actually say. Don't just dismiss it as propaganda because they've spent a lot of time carefully honing those adverbs.

Compare it to what they do, and then when we interact with them, regularly compare the two and say, "Well, you did this, but you said that." Because

there's nothing in my experience with Mashat Tien and other Chinese military officials that I've dealt with pulling out their copies of the U.N. Convention of the Law of the Sea and lecturing us. Nothing shuts them up faster than when you've actually read the relative Chinese documents and you, in fact, call them out on the contradictions between those documents and their own behavior. At that point everybody just says, "It's time for lunch."

And finally, what I would say, the other thing that you don't do is unfortunately what we saw in the aftermath of the conference that Ken mentioned, which was the Chinese -- the Internet censorship czar, Mr. Lu Wei, when he went out to the West Coast this week. And instead of being treated as the authoritarian enemy of Internet freedom that he really is, was treated to a display by Mark Zuckerberg and the people at Facebook and the people at Google that to me was obscene, if almost pornographic. The image of Mark Zuckerberg bringing Lu Wei into his office and admiringly showing him that he has one of Xi Jinping's writings books on his desk as a guide to socialism and that he gives these out to other tech entrepreneurs as a guide to understanding Xi Jinping's vision of socialism is about as, you know, sort of -- one muggles to think of the word for it, but it's one of the more sort of weak-kneed approaches to a global information society that I could possibly imagine.

Thank you very much.

(Applause)

MR. POLLACK: James, thank you. And thanks to Ken as well. The words have leapt out from both presentations, questions of schizophrenia, references to contradictions. And so if we're all being good students of Chinese political theory, we'll go back to Mao and ask whether the contradictions are antagonistic or non-antagonistic. I think I know the answer. I'm also struck, given the sobering arguments that Ken has

made about what's in that iPhone of mine, that if I'm imagining it from the point of view of those trying to exhibit maximal control of the Chinese system, I would say that some find that a good thing and some probably find it a not so good thing. It's certainly information that's elicited that you'd like to have, but a lot of things you may not want to know about. But I'll leave it at that.

Since I know our time is short, rather than my make a whole set of comments, I'm going to open this up because we have a rare opportunity with three people who really have studied seriously these issues. So I will open it up for discussion, for questions from the audience. Please identify yourself. Please a question, no statement. And keep it as short as you can.

Yes, I see a hand up standing in the back of the room.

MR. WOO: David Woo, former member of Congress.

The question has to do with Dr. Austin's comment that China has a lot invested in the existing world order, and in my interactions with young people in China and with young Chinese students here, there's a lot of push to upset the apple cart. And you might say that maybe adults have cooler heads, but in my observation of U.S. policymaking, in that small room you get a lot of contradictory views hashed out. Sometimes voices are raised and not quite rational decisions come out. Is there concern on your or the panel's part that China's policies might hurt its own interests, our interests, and contradict this rational view of decision-making?

MR. POLLACK: Should we start with our author?

MR. AUSTIN: Well, thank you very much. Very good question. One could add to the aspirations of youth to upset the apple cart. The aspirations of leading figures in the Chinese People's Liberation Army. There are some rather disturbing statements there about how Okinawa doesn't really belong to Japan. That would be a

major upset of the apple cart.

And I think what we're seeing is a very unusual contest which from time to time gets out of hand in a pluralistic society as China has become, and it's very different from our pluralism. All sorts of opinions are surfacing. I think at the end of the day what we've seen in the last two years, the last week of September, Xi Jinping had to do some very heavy work to slap the PLA into place after they, yet again, provoked an incident while he was in India one year after they'd done the same thing with the prime minister. But there were conciliatory efforts on all three fronts -- China-Vietnam, China-Japan, and China-India -- in those last two weeks of September, and that's a situation I think we're going to go forward with is this policy entrepreneurship of our key sectors in Chinese government, whether it's the oil sector overseas, oil sector perhaps related to the oil rig off the Paracel Islands. And then occasional efforts by the leadership to pull them in. I think that's a more unstable situation than we had before.

Let me stop there.

MR. MULVENON: I am struck. I mean, I think Ian Johnston, in particular, has done some very, very interesting work to show that by almost any metric you can come up with, that China is status quo rather than a revisionist power. But I guess the irony for me is that it seems like many of the things that China is doing, particularly in the international sphere, in many cases with all the right intentions, are, in fact, achieving the opposite, which is that it is coming across as a revisionist power because perhaps the existing power structure is not as accommodating as they would like. So I think structurally, they're very focused on status quo across a wide range of dimensions, but we may not get there nonetheless because of the way in which it's being pursued.

MR. POLLACK: More questions? Yes, right here.

QUESTIONER: (Inaudible), China Daily.

I have two questions. A key issue between China and the U.S., I mean, and Canada meeting recently, obviously, I mean, what, you know, you all mentioned cyber espionage. These Chinese believe, I mean, after the Snowden revelation, the whole world knows, you know, the U.S. has the largest capacity and was able to sort of steal more information from any other country, from China included, than any other nations. I mean, including hacking into Huawei Chinese University. This is all according to Snowden. But the U.S. obviously is arguing China is doing this Internet, cyber theft of intellectual property rights.

So in your view, what should, you know, should be the rule? Should I be allowed to hack into the White House, not the Commerce Department? You know, obviously, what should be the rule? Thank you.

MR. LIEBERTHAL: Well, we may have three different responses here.

The U.S. has sought to make a distinction and to get China to take that distinction seriously. The distinction between espionage for military, strategic, local, whatever purposes, which all governments have always done. The cyber arena provides additional tools for that, and we just assume all governments will use that as best they can. That's on the one hand.

On the other hand, there is the theft of proprietary information. It may be technology, it may be spy chain management information. It may be negotiating points, bid plans and auctions and so forth. And then providing that information to your own pertinent firms so that they can then compete better with the firm from which you stole the information. The U.S. Government is barred by law from providing competitive information, and so we don't do it. It isn't that we don't intrude on any enterprise information. I assume we do that on a fairly large scale, but we don't turn it over for

competitive purposes to our own companies.

Now, how many countries follow the same rules as the U.S. on this? My guess is extremely few. Than why particularly go after China on it? Because China seems to do this on a scale that is absolutely in a category by itself. And I suspect what we're really trying to do -- we'll never say it, but what we're really trying to do is to get China to do it no more than most other countries do it, in no small part because, remember, you have a president that came into office here with his number one task being to revive the American economy from the depths of the global financial crisis, and especially within that, to increase jobs. And China's theft of proprietary information and using it to undermine U.S. competitiveness has directly made it more difficult for the president to get out ahead on that issue. And that's his number one job. So I think that's been taken extremely seriously.

And then when the Chinese side says, you know, we indicted five Chinese military officers for hacking, regardless of one's views on whether that was a good thing to do or not, the Chinese response is, "Why didn't you raise this privately? You've never given us any evidence on this. You've never made this accusation in any detail privately." And that's simply false. We've done it for years and we've built up to Sunnylands and Sunnylands is one of the president's top priorities and what he laid out for President Xi. And so to (a) deny that they do it at all, that China does it all, and (b) say, "Why didn't you raise it privately," is a level of denial that frankly doesn't sit well given the phenomenal amount of information available on this. So I think that's why it gets singled out.

MR. POLLACK: I'm wondering whether any of our panelists would have a thought as to why, given Chinese practice, clearly there is not the same distinction made that was made in the United States Government. The presumption is anything

seems fair game as long as you have the tools that enable you to do it. So is it simply sheer, what I'll call technological opportunism, or is there something more about this that evidently the Chinese do not make a distinction between, in this fundamental way that the United States government does?

MR. MULVENON: I think it has a lot to do with the arguments Greg makes in his book. First of all, you know, when you have a situation in which you have an economy that's still much more state-centered in terms of strategy, when you have large state-owned enterprises that can be the beneficiaries of this, there's not the same level of separation. And so the same actors in PPPLA or in the MSS that are carrying out this activity, it's not that difficult to find a pathway to a lot of these key state-owned enterprise actors that could benefit directly from the information. A lot of the countries we deal with around the world, they have a single-state telecoms country, a single-state oil company, a single-state chemical company. It's obvious who to share it with.

The argument that I've made to the Chinese side in the dialogues is I try to make a very practical argument. I say, "Look, if NSA was to steal Wu Wei's latest networking technology in 2015, the real problem we have, and the reason why we're legally precluded but there's also a practical consideration, who do you share it with? Do you give it to Cisco? Do you give it to Juniper? Do you give it to Cisco and Juniper? Do you give it to any one of a dozen networking startups in Silicon Valley?

Here's the unique thing about our legal system -- if anyone of those companies finds out that they didn't get it, they actually have legal standing with the Justice Department to file an antitrust lawsuit against the U.S. Government. That does not exist in other countries' legal systems. And the Chinese side weaves that away and says, "Well, you know, your government should be able to override you legal system just like we do." And we're like, "No, you know, our legal system, you know, holds its own

weight there."

But the other issue is to say, as Ken did, allegedly going against Petrobras or foreign companies. Policymakers in the White House and the Commerce Department are the places. You know, have needs for strategic economic intelligence about what is going on in the global economy, what is going on with foreign companies. That is not the same thing as giving it to Exxon Mobil. And that is just a distinction that Ken and I in particular are just not going to stop talking about, no matter how many times the Chinese side says that it's a false distinction.

MR. POLLACK: Would you want to join in?

MR. LIEBERTHAL: Yeah. A good set of questions.

I, as James said, took the effort to read the documents on this one, and one of the really interesting things about the indictment -- there are many interesting things about the indictment which are a little bit counterintuitive. One is that there are only two charges of industrial -- two counts of industrialist but not (inaudible) counts. And they involve a company Westinghouse. Westinghouse is so disadvantaged by the Chinese theft that it's just about to sign a deal for $26 billion and 20 new reactors with China. So I'm not sure what the disadvantage is. One of the really interesting things in the indictment is it says that in respect of Westinghouse, unit 6138 formed an illegal relationship with an unnamed SOE. So the indictment says that what the Chinese unit did was illegal in China, I suspect. Maybe it was illegal in the United States, but the question is, is it illegal in China? I haven't been able to find that out. But the institutional setting in China is not conducive to good policy on this, not least evidenced by the fact that Jay Yung Kang, who ran all of the intelligence agencies or had this oversight, you know, is now under investigation for serious corruption. So that opportunity for corruption between PLA intelligence units and corporate entities in China is pretty high.

MR. AUSTIN: And it's also difficult for us to have serious dialogue when the Ministry of National Defense comes out at their official press conference and their response to the APT1 report at unit 61398 is to say, and I quote, "There is no unit 61398." I mean, it's Kafkaesque.

MR. POLLACK: Yes, right here.

MR. GARVEY: Patrick Garvey with CSIS.

Are we to assume then that cyber theft is policy?

Second, two of you mentioned the concept of quanta computing. How have they made such leaps there given Greg's tenets?

MR. LIEBERTHAL: Well, let me do the one I know about, which is not quantum computing; is cyber theft policy? It's clearly China policy to suck up all of this information. They don't have highly developed and highly differentiated policy of the sort that's developed or the intelligence community in the United States and Australia. This is one of the most sensitive political environments in all of China. There is nothing more sensitive than what the intelligence agencies do, especially in an environment post-Bo Xilai, where these very same intelligence agencies were implicated in monitoring Hu Jintao.

So we've got this awful institutional mess at a time when Thomas Donilon was issuing in public these demands a year or so ago, 18 months ago. Then there's the indictment. Well, it's very hard for Xi Jinping to burn political capital by bringing the PLA intelligence agencies to heal when he depends on them for his political survival. He's investigating most of their leaders for corruption, and I do mean most of their leaders. He's not going to charge all of them, but it's a very tough environment. And one of the evolutions for China is to bring its intelligence agencies into line. And we know so little about that we don't know.

James, can you answer quantum computing?

MR. MULVENON: Well, I mean, also there are a range of documents that describe in cases where you can't get technology through transfers from multinationals operating in China where you have leverage on them with access to the Chinese market for some of the established R&D labs and the like. There are classes of technologies that simply don't have analogues in the Chinese economy. You know, military specification, traveling wave tubes, and things like that. And there is specific discussion about other means, and we may those out in our book on Chinese industrial espionage. Other means, it doesn't black or white say, "Please use cyber espionage." I would just highlight that the shift to cyber espionage against commercial interests in roughly '05-'06 lines up pretty nicely with the publication of the 2006-2010 mid- to long-range S&T plan. As an intel officer, I don't generally believe in coincidences. And I really think it reflects the relative ease with which you can exfiltrate large volumes of highly sensitive information out of companies that are poorly protected. Whereas, before, China's only recourse would have been to run a very complex and very risky human operation that would, in many cases, result in people being perp walked in front of the LA Federal Courthouse.

MR. LIEBERTHAL: At least some of this clearly is also just simply corruption.

MR. MULVENON: Opportunism.

MR. LIEBERTHAL: Opportunism. You pay for X kind of information and it's delivered.

MR. MULVENON: Right opportunism.

MR. LIEBERTHAL: On the quantum computing, I'm going to turn it over to James, but I have seen some description of the magnitude of the Chinese effort on this

and it's very wide-ranging. It's not all in one unit. You know, we're just going to give them money and resources and stuff. It is a multifaceted effort to master this. Let me say the U.S. also has a multifaceted major effort to master it. This is in some ways a Holy Grail kind of thing to get to.

MR. MULVENON: Well, with respect to quantum, I mean, I don't want my comments to suggest that there are not areas in which Chinese scientists have made fantastic advances, simply by dent of their hard work and their imagination. And I always tell people in the U.S. Government at Huawei. I said, "Yeah, they may have started out as a company that stole designs for PBXs and things like that, but they are now a legitimate, state-of-the-art world leader in 4G LTE and a bunch of other critical technologies. How they got there, you know, that's up for debate, but China, you know, China developed an atomic bomb, a hydrogen bomb, put a satellite in orbit. I mean, a lot of other things going on. So to say that there is a state strategy to be able to jumpstart indigenous innovation through foreign acquisition by any means possible is not to diminish legitimate scientific breakthroughs that they have made.

MR. POLLACK: Wouldn’t this give the relevant Chinese entities, as they develop their own expertise, much more incentives to try to protect where in the past they have tried to steal?

MR. MULVENON: Well, this is the argument we've always made about intellectual property in China is that China will protect intellectual property when it has intellectual property to protect. And we do see an interesting phenomena in the Chinese patent world of patent trolling on a very large scale in China where you can take foreign patents and then take the text of them and then license them as Chinese patents and then force multinationals basically to buy your own patent back from you, which is on the scale of the enormous amount of plagiarism we see in the Chinese academic and

scientific community that is really a national scandal as well. So, you know, breakthroughs in quantum paired with academic plagiarism. That's one of yet another one of these dichotomies I think that Greg's book brings out in pre-stark relief.

MR. LIEBERTHAL: And just a 20 second footnote on quantum computing. Google it to see the number of joint China-American congresses there are on quantum computing. I mean, the interchange between the United States and China in all of these areas of advanced science is very high. I mean, we hear about the stories of it being closed off in this or that area for NASA or whatever but, I mean, this is like fluid dynamics. It's not sort of two separate words, really.

MR. POLLACK: Yes, in the back of the room there.

MR. HUTSELL: Yeah, hi. Mark Hutsell, German Marshall Fund.

I think I've already had the answer already to my question here given throughout the day, but are there any real debates going on right now in China between the policymakers, let's say in the government, and then with the military on where they want to advance and where things are going? Are they so intertwined where there's never really going to be a conversation then kind of change that needle to either advance China in with cyber policy and sort of move them forward? Is there any debate right now between the military and policymakers?

MR. LIEBERTHAL: That's a great question. I can answer it from my part very quickly.

When Xi Jinping made the announcement -- I think it was in August -- that China needed to do more in the military sphere, he said we need to abandon mechanization. He didn't use these words, but he basically said we need to drop the blinkers of mechanization. And for those who study this thing -- mechanization was where Chinese PLA was going from about 1995 to about 1999 or even beyond. But what

he's saying is that you guys just don't get it. You want this jewel track policy, mechanization plus informatization, like industrialization and mechanization, but sorry, it's all informatization. We've got to become a cyber-power. Forget the armored personnel carriers. Let's build the cyber assets we need.

MR. POLLACK: Yes, the woman right there.

MS. KENYA: So a few weeks ago China has --

MR. POLLACK: Identify yourself, please.

MS. KENYA: Elsa Kenya.

A few weeks ago --

MR. POLLACK: Your institutional affiliation?

MS. KENYA: I'm a Harvard student currently and intern at the Institute for the Study of War.

A few weeks ago, China hosted its first World Internet Conference, which in and of itself might be considered something of a contradiction. And at this conference, Chinese leadership was pretty aggressively promoting the concept of cyber sovereignty or Internet sovereignty, which seems not to have been terribly well received among attendees. But it seems that over the past few years China has been highly active in Internet-related diplomacy and at conferences like WCA 2012, China's views seem to have gained some traction among a certain constituency of countries. And recent developments like a Chinese national becoming secretary general of the ITU, do you see these -- do you see Chinese views in cyber sovereignty as gaining traction and as posing some degree of threat to U.S. interests? Might you say that the Chinese leadership, if they can't adapt to the Internet as it is, is trying to -- could be trying to change the standards under which the Internet is run, or is there some degree of alarmism in discussions (inaudible)?

MR. AUSTIN: It's an issue that I spent a lot of time looking at. It's a great question. China, I would argue, in the vast majority of the countries in the world, have a very different view of Internet sovereignty than traditionally, for example, Secretary Clinton's State Department had, which was that China -- and I think very presciently -- looked out at the architecture and said, "Okay, every client, every computer, every router, every switch in the architecture is actually located within the sovereign boundaries of a nation state and therefore governed by its laws or travels on submarine cables or satellite connections that are owned by companies that are incorporated in countries and therefore, governed by their sovereign laws. So even though my name is on a CNAS report about the global commons, in a chapter on the cyber commons there is no commons in cyberspace. The architecture itself fits very neatly into traditional Westphalian notions of sovereignty, not like air and sea and space and other areas. So they're on high ground there in terms of making that argument.

Where they've run into friction with the United States is that we traditionally, in our own Internet development -- our own Internet development was a very sort of crypto-punk-libertarian-organic kind of thing where we allowed organizations, nongovernment organizations dedicated to privacy and other things, to have an equalcy to the table. And basically, Beijing's argument right now is because such a huge percentage of the global economy is now riding on the Internet, it's much too important to be allowed to be left to a bunch of Birkenstock wearing long hairs who want to be anonymous on the Internet and do cost play. It really needs to be controlled by the adults who are managing the global economy, and those guys are just getting in the way. The funny thing is I deal every day with parts of the U.S. Government that also share China's sovereignty-oriented view of the Internet -- DHS, NSA, DOD -- who believe that there are, in fact, national boundaries. There are networks that need to be defended that are

American, et cetera, et cetera.

But what we see because of the strength in some cases of China's argument and also because they have bandwagoned so many other countries together, is that we are, in fact, losing the battle on Internet governance. WCA was a disaster in Dubai in terms of U.S. position. We got rickrolled pretty hard at that meeting. But, you know, you mentioned the World Internet Conference. And this is the key distinction. You have a conference sitting in basically a technological Potemkin village, which is wired from top to bottom with surveillance, with military and MSS and MPS units driving around operating stingrays, surveilling every cell phone in the place, while it's crawling with goons from Belarus and Russia and China and all these countries that don't give a fig about Internet freedom. You know, the U.S. Government didn't have anybody of any note there other than the embassy staff. It was really a discussion among the sort of repressive Internet class. And when the Chinese Government, in classic fashion, at 11 p.m. the night before the conference ended, tried to slide a heavy-handed declaration, pushing their Information Code of Conduct under the door saying if you don't submit your changes by 8 a.m. tomorrow morning we're going to publish this as the consensus of all the attendees, you know, some people in the room who were there got up very early and cornered Lu Wei and said, "You've got to be kidding me. This is not Internet governance. This is not global democracy. This is not the way we do business." And that to me, that episode is such a microcosm of the conflict, of the problem between the two sides.

MR. POLLACK: We have time for just one more question.

Yes, right here.

MR. KANE: Tony Kane from American Councils for International Education.

I'd like to ask for a follow-up on the comment that China is so committed

to moving forward and that Xi himself is taking charge and the idea that they're falling backwards. And if you would look forward, whether this tendency is likely to keep going in the direction it's going now or whether at some point you think Xi will be able to reverse it. Because to me it's reminiscent of the days in the Maoist era when the chairman said something had to happen so that people were more anxious to say it was happening than to make it happen, so that in fact, less was happening instead of more.

MR. LIEBERTHAL: Well, that's a very good analogy and a good question.

There are many positive things happening, and the internalization of Chinese universities is one. The internationalization of the Chinese private sector is another. The shrinkage of the Chinese Communist Party's area of control is another.

On another slightly different note, something in a sense relating to the Internet question, there are this group of people in China who think very differently from the leaders and who have been advising them very differently. And there was a woman who was at a pivotal role at vice minister level in all of this who has published a book on this and there's a quote from her in my book. She could not be more critical of the Chinese leadership for its lack of support for creativity, innovation, and ethics. There's also an excerpt from a statement by Jung So Min -- of a speech by Jung So Min. "There's something wrong with the Chinese people. They're not creative. We're not brave enough."

So there has to be a crisis. I think my book concludes with the note that there really has to be a crisis if there's going to be a breakthrough. They can't really have an advanced information economy and society without giving up power in the universities, without freedom of information. You just can't have it.

MR. POLLACK: I want to thank all three of our speakers today,

especially Greg Austin, who, of course, stimulated this by the publication of this important new book. I have no doubt that a lot of us are going to be reading it carefully. As some of us try to come to terms with technology in a world that, at least among some of us older folks, is almost beyond comprehension.

But thank you very, very much for your time. And thank you to Greg.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

)Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016