THE BROOKINGS INSTITUTION

FALK ROOM

# CENSORS AND HACKERS:

# THE ROLE OF THE INTERNET IN

# U.S.-CHINA RELATIONS

Washington, D.C.

Monday, April 19, 2010

PARTICIPANTS:

**Introduction and Moderator:**

RICHARD C. BUSH
Senior Fellow and Director
Center for Northeast Asian Policy Studies
The Brookings Institution

KENNETH G. LIEBERTHAL
Senior Fellow and Director
John L. Thornton China Center
The Brookings Institution

**Featured Speakers:**

EMILY PARKER
Arthur Ross Fellow
The Asia Society

JAMES MULVENON
Director
Center for Intelligence Research and Analysis
Defense Group, Inc.

* * * * *

PROCEEDINGS

MR. BUSH: Good afternoon, ladies and gentlemen. I'm Richard Bush, the director of the Center for Northeast Asian Policy Studies here at Brookings. I am joined by my colleague, Ken Lieberthal, the director of our John L. Thornton China Center in welcoming you here today.

I have to say that we're really glad to see you. Ken and I walked into the room where this was originally going to be held and saw absolutely no one. And so we went into a mild panic and I'm glad I took all my blood pressure medications this morning.

But we are glad to see you. We're even more glad to have Emily Parker and James Mulvenon speak to us today on the issue of "Censors and Hackers: The Role of the Internet in U.S.-China Relations." I think that this is a subject that obviously is already moving to the center of U.S.-China relations. I think it's going to be with us for a long time.

I recall about 10 years ago when there was fond hopes about the Internet transforming China because people could use the Internet as a weapon against the State. It turns out the State is pretty good at using sort of its own weapons against the people in this regard. Also as we understand, the Internet can be used by people in one country against other countries. And it's not just the State using it; it's the people as well. So this is really interesting. It's going to become even more interesting.

Each of our speakers will speak for about 20 minutes and then Ken will moderate what I think will be a lively discussion. So without further ado, Emily.

By the way, Emily is an Arthur Ross Fellow at the Asia Society. She worked for The Wall Street Journal for six years; three years of those in Hong Kong where she covered both China and Japan. With that --

MS. PARKER: Good afternoon, everybody. Thanks to the John L. Thornton China Center and the Center for Northeast Asian Policy Studies for having me today. And it's wonderful to be up here with James, who is extremely knowledgeable on this topic.

So I think Richard actually brought up some of the key -- some very important points. And the one point that I want to talk about is, as Richard said, there's been a real shift in the conventional wisdom here in the West, and probably in China as well, over the power of the Internet to transform Chinese society. I would say even from around 2004 until today, I think people generally see this issue very different. I think when, you know, if you looked at this five years ago, there were a lot of people thinking that the Internet was really going to change things in China. It was going to deliver freedom of speech, freedom of expression, freedom of assembly. And now we have a slightly different take on that. So I want to just sort of give a general -- my view of this evolution over the past few years.

So I started covering China and the Internet in around 2004. I was in Hong Kong and I wrote a column for The Wall Street Journal called "Virtual Possibilities: China and the Internet." And at that time it was sort of part of a general media, you know, Western media *zeitgeist* about how great the Internet was in China. We knew that it was a cat-and-mouse game. You know, we saw, okay, there's the government on one side and then there's these wily Chinese netizens on the other.

But I think generally we all thought that -- we were all pretty optimistic about it. We were optimistic about it because it just seemed at that time -- you know, there was still the Great Firewall. There were still tens of thousands of Internet police. But what I discovered in covering this topic was that almost any information that wanted to break through could in some way. So every time -- and that was the point of my column. Every time the government tried to block a piece of information, people would find a way to get it out. And they did this in all sorts of different ways. I think, you know, it was much more primitive then. One of the main ways that people tried to get around electronic filters, for example, would be by misspelling a Chinese word or sometimes putting asterisks, you know, in between or sometimes putting Roman letters. They would just do very simple things to disguise sensitive terms, and in doing so would be able to have these very lively discussions about even the most sensitive topics.

So, you know, we were watching this. We saw online petitions. There was an online petition, for example, for Jiang Yanyong, the SARS doctor, who blew the whistle on SARS. That may have led to his release from jail. You know, we saw -- we all saw how there were these very specific events that were pushing information out into -- just into the world. So this was sort of 2004-2005.

When did we start to worry about this? I mean, if you look at this as a battle between, you know, the netizens on one side and the government on the other, when did the public perception start to shift in believing that the government was winning this war? I think a big part of it was when we started to see U.S. companies falling in China. I think, you know, if we all believed in the beginning that, okay, the netizens are really using the Internet to increase freedom of speech, we believe that U.S. companies, U.S. Internet companies, were helping in that way. They were helping promote Internet freedom. And I think, you know, one after another, first of all, I mean, I think the most egregious example was Yahoo, which famously provided information to Chinese authorities that landed a Chinese man called Shi Tao in jail. And I think that was when people started questioning, you know, what is really the role of these U.S. Internet companies in China?

Then there was Microsoft. Microsoft, you know, was widely criticized for closing a Chinese blog. Then there was Google. Now, Google -- when Google entered the Chinese market in 2006, you know, I was still there at that time and I think we were all very -- we all had mixed feelings about it because Google was very up front about the fact that it was entering China, but that it was going to be self-censoring its own search results. And I think, you know, the journalistic community was really struggling with how to deal with that because, you know, Google's argument was if we don't do this, if we don't comply with Chinese law, then we are not going to be able to enter the Chinese market. And I think the general feeling was, okay, more news is good news. And so I think people generally bought Google's logic; was that, okay, we're making some sort of compromise, you know, to enter the Chinese market. You know, they would basically -- when you search for a sensitive term, Google itself would not give it to you. And they sort of convinced the world that that was the right strategy.

Now, as we all know, a few years later, Google has departed -- basically departed mainland China, moved over to Hong Kong. And I think in some ways it's an admission that that strategy didn't really work. Now, Google -- and I think James may get into this more in detail -- Google's only concern in China was -- it was not only censorship, but had other concerns as well. But I think, you know, Google's decision to close down China.cn was in some ways a tacit admission -- or actually rather an open admission that, you know, its attempt to increase the -- increase information in China has not succeeded.

So I think the question is where does that leave us? I think, you know, the succession of events -- and it's not only Google and it's not only Yahoo and Microsoft. It's also, you know, the fact that the Chinese government has shown an amazing capacity to keep pace with Internet dissidents or netizens in general. I think, you know, surveillance has gotten much more extensive. It's gotten much more sophisticated. We're still seeing Internet dissidents getting arrested and going to jail. So I think a lot of people underestimated, like, how well China would sort of handle this Internet -- this new Internet threat.

So, again, where does that leave us? I think, you know, it leaves U.S. policymakers in a bit of a bind for various reasons. You know, the question is that if it is a

U.S. foreign policy goal to like promote Internet freedom in the world, how do we do this? I mean, how do we do this in China? And I think the Google model, which is basically al U.S. Internet company coming into China and saying, you know, we are going to like bring more information into China, I think right now there's limits to that strategy and I think we need to sort of start thinking about other strategies.

I think also that in terms of, you know, Google has been applauded for taking a principled stance on Chinese censorship. That's great, but I think in the short term it's unclear how Google's move will really increase Internet freedom in China. It probably won't. It's probably going to be about the same over the short term. I mean, basically what we're having is Google.cn, you know, which was first censored by Google itself has now moved over to Google.com.hk, which is basically blocked by the Great Firewall of China.

So on balance we're not seeing a huge change in the Internet landscape in China. And I think also my sense of the Google situation is that, you know, it's been a real tense point in China-U.S. relations, but I think it could still get worse. I think it could get worse because -- if the U.S. doesn't play its hand correctly. Right now I think public opinion in China for those who even know what's going on between Google and Beijing; there is some sympathy for Google in China. There's some sympathy, for example, among academics who, you know, feel that Google is better than Baidu for, you know, getting certain terms. There is some sympathy among, you know, obviously, you know, more reform-minded young people who just think this is a terrible thing. I think, you know, the -- and, of course, there is nationalist sentiment in China as well. People saying, like, how dare this foreign company do this? You should really comply with Chinese law.

But I think, you know, the sentiment is mixed. I think that if the perception shifts toward Google being seen as a foreign bully or a pawn of the U.S. Government, then we could see a really dramatic shift in Chinese public sentiment. I think you would see the media portraying it that way, and I think, you know, as we've seen over the past few years, Chinese nationalism is not only directed from the top down. I think, you know, once -- I think it's very deep in the Chinese psyche, this idea that China has been humiliated through history and, you know, been bullied. And I think, you know, we need to avoid that at all costs. So, I think, we really want to depoliticize this issue because once this becomes sort of a war of ideas between China and the U.S., and the U.S. trying to impose its values onto China, I think this could become a very messy thing.

So one of the things that I've been talking about recently and one of the things that I've been sort of studying is a different approach. It's something that I refer to as twitter diplomacy, as opposed to Google diplomacy. I mean, Google diplomacy I would define as, again, coming into China and trying to bring information into China. I think now the more practical model is for U.S. companies is to focus on, you know, providing the best types of services outside of China and focusing on how we can get the Chinese to come to us, you know, as opposed to going into China and bringing the information into China. And it's sort of a subtle difference, but I think it's something that's more likely to work.

Now, let me explain a little bit about Twitter in China and why I think it's important. Twitter, like YouTube, like Facebook, is blocked by the Great Firewall of China. I'm sure many of you are familiar with this terminology. Great Firewall, just, you know, generally speaking, is what's used to block sensitive content from international -- from foreign websites. Now, Twitter, YouTube, and Facebook are blocked completely. And the reason is because they are seen as organizational tools. I mean, that's one of the main reasons. And I think this is a very important thing to understand why the Chinese government sees the Internet as a threat. I think here people tend to talk about the Internet in terms of freedom of speech, spreading freedom of speech. I think what's of much greater concern to the Chinese government and to governments worldwide is freedom of assembly, not freedom of speech. I think if you look at what makes governments nervous, it's not, oh, I got this article out onto the Internet. Oh, I said this controversial thing. It's I managed to organize. I managed to form a group. And I think that's really, really important to understand in terms of what the government is nervous about.

So Twitter especially is seen as a mode of organization. And, you know, if you look at, for example, a very simple example is the events in Iran. Twitter was, you know, used to get people together. And so I think that's something that China really worries about.

So anyway, these three things have been blocked. And Twitter, however, if you talk to some of these, you know, very cutting edge Chinese netizens who have been doing this since, you know, 2004 or earlier, Twitter has an almost religious following among these people. I mean, it's really incredible. I mean, they really -- I recently moderated an event between Jack Dorsey, who is the co-founder of Twitter, and Ai Weiwei, who is sort of an artist-activist, who came from China basically to deliver a message to Jack about how important Twitter was to Chinese netizens. And he actually told Jack, you know, we think of you as a god here in China.

And it's a little bit over the top, but it's kind of -- you will see that if you talk to these people. And Ai Weiwei estimates -- now, again, this is his estimate. I'm not even sure where it comes from. He estimates there's as many as 50,000 Twitter users in China. Now, when you're talking about 400 million or so Internet users, this is a tiny number. I mean, I don't want to overemphasize how large this number is, but it's still significant. It's not nothing. I mean, it's 50,000. It's small, but it's not nothing. And again, Twitter hasn't confirmed these figures because it's very hard to tell.

But how do people use Twitter? It's still 50,000 roughly, we estimate. They use it very simply, it's not difficult. I mean, in order to use Twitter in China you basically have to get over the Great Firewall. That's, you know, so because it's blocked. And, you know, for example, if anyone here were to just go to China today, go to a normal hotel and log onto Twitter.com, you would get an error message.

So what do you do? I mean, there's, you know, there's various different ways. The main things that people have been using and that they've been using for years are largely proxy servers or virtual private networks. Virtual private networks are, you know, you can buy one for $39.99. I mean, you can just buy one off the Internet. There's all sorts of different models.

Now, VPNs, people ask the question why don't they shut down VPNs in China? The reason is because foreign businesses depend on VPNs. You know, so these are tools that already in China that are used by foreign businesses. You need them, for example, for secure bank transactions. But the Chinese -- you know, other Chinese people managed to use them to get access to sites that are blocked.

There's another reason why Twitter is easily accessible in China. And it's not -- it's only for, you know, VPNs and proxies are used to just basically circumvent the Great Firewall. There's actually an aspect of Twitter's design that makes it easy to access in China. And I think this is a very interesting thing. Now, I know that Twitter is a very different kind of service. So you can't apply this to every, you know, to every possible tool. But, Twitter has basically an open API, an application programming interface. And when I, you know, started looking into this and asking these Chinese Twitterers how do you use Twitter, they all were talking about Twitter's API. And I'm not a tech person. James here is much more of a tech person than me, but you know, I slowly grew to understand what that means.

Twitter's API basically means that coders elsewhere that outside of Twitter can offer up Twitter feeds at their own URLs and the government has to chase those down one by one. So basically the idea is you can -- I mean, to put it simply, you can -- because of the way that Twitter is designed, you can get tweets and you can tweet yourself on sites other than Twitter. And that's a part of Twitter's design that has no political -- no obviously political motive. It's something that Twitter just designed because they wanted to spread Twitter worldwide and have coders and have people use it as easily as possible.

Now, I think somewhere in there, to me, seems like a really good option for us because if you look at that, it's sort of -- it's not a political response. It's something that Twitter did just to make Twitter the most, you know, as easy to use as possible. And it works, but it's not, you know, it's not as politically -- it's not as politically sensitive as, you know, circumvention technology. It doesn't involve, you know, U.S. officials having to be seen as, like, lecturing China. And I think, you know, so some of the things that I think we do want to think about, and I think people are thinking about this right now in government and in the private sector, is how private companies can design tools that will make it as easy as possible for the Chinese to access them without having an overtly political, you know, an overtly political motivation.

And, you know, the reason again this brings me back to the question of, you know, the reason why Twitter is important in China, again, I'm sure some of you are asking how can it matter? How can something that 50,000 people, if that, have access to matter? It matters because, again, it's back to this freedom of assembly question which right now in China is more like freedom of virtual assembly. It matters because, you know, if you talk to a lot of these people, you know, all these sort of netizens who are at the forefront of this moment, and you ask them why is the Internet important in China? And I've been asking them this now for five years. Why is the Internet important? If you're going to put something out and it's just going to get deleted, if this website is just going to get blocked, why does it matter? And what one of them told me and which has always stayed with me because it seems like a very smart answer to this, is he said because now I know who my comrades are. And basically, you know, what he’s saying is that for a lot of these people, they grew up feeling that they were very alone in how they saw the world. They were very -- they felt very alienated. And what the Internet has done, and which it does in countries all over the world, is it has allowed for a congregation of like-minded individuals.

And I think Twitter is a very decentralized type of organization, you know. It’s not -- it doesn’t have, like, one leader. It doesn’t have a chief. It doesn’t have, you know, it’s not the kind of thing like a petition or an open letter. It’s just sort of like a very widespread-type of organization with no clear center. And I think that’s why -- and when you talk to these, again, when you talk to these Chinese netizens and you say, well, why does Twitter matter if there’s so few people here? They see themselves as -- they’ll say because every movement needs leaders and they see themselves as future leaders. And they see themselves as finding like-minded individuals across the country that they never would have had any means of locating before.

So I think, you know, I think, again, that’s something that I think this kind of technology, you know, Twitter will likely disappear or will likely be -- at some point it will likely be surpassed by some other faddish technology. I don’t think -- the point is not Twitter itself; the point is that we need other types of things that will serve as a catalyst, you know. Basically a catalyst for organization. A catalyst for change. As opposed to we’re going to try to sort of insert information into China.

Again, I think that I remain optimistic about the Internet in China. I think that, you know, even if people are -- even if that is not the conventional wisdom right now, I think if you go to China and you talk to people and you ask them, you know, the Chinese people on the ground, what is your view about the outlook for Internet freedom in China? They will usually tell you that the short term looks bleak, but the long term is quite bright. And I think that we need to focus on here in the U.S., you know, if we are serious about, you know, promoting Internet freedom around the world or making that part of the U.S. brand identity, I think we need to think long term and we need to think of sort of pragmatic solutions to this problem. And I think technology companies, you know, having technology companies lead the charge is probably in some ways the most pragmatic long term response.

Thank you.

MR. BUSH: Thank you very much. Very interesting.

We now turn to James Mulvenon. He's the director of the Center for Intelligence Research and Analysis at the Defense Group.

James.

MR. MULVENON: Thank you, Richard. Thank you to Ken Lieberthal, my sensei so many years ago at the University of Michigan.

Now, not surprisingly given some of our, you know, military intelligence industrial complex customers I had to clear my remarks today with lots of different people. But one thing I didn't worry about was clearing it with the Chinese government because I figured they probably have already seen my presentation in multiple forms via access to my computer or various other things. So I just really feel like I can dispense with that and go to bed and not worry about that.

What I'd like to talk about today are some of the higher level strategic issues that I've certainly been thinking about recently as I try and process things like the Google-China dispute which swallowed basically the first three months of my life in 2010. And some of the -- frankly, some of the hard questions that we're dealing with now on a broader level in the cyber agenda -- General Alexander's testimony the other day before Congress being the best example of this -- and how so many of these examples can be illuminated by the disputes that we have with the Chinese or the challenges we have from the Chinese side. And so I'm just going to try to weave those together.

But I'd like to start at the strategic level and work my way downwards. The most important thing is that the stakes in my view on the cyber security front are getting higher every day. And what do I mean by that? I mean we are witnessing a pretty dangerous convergence in my mind between on the one hand our increasingly global dependence on the network for everything. Now, some countries are more wired than others. You know, the reason why the Estonia attacks were in some cases so threatening was because they had literally gone to an E-banking posture. I mean, unlike -- my parents still like to go into the bank and talk to the teller every week and they know they're getting charged for it and they don't care because that's the way they always did it. But everyone in Estonia did E-banking. And so when the E-banking was cut off, this was actually a fairly -- a dire situation for them. And frankly, it's a harbinger of our future. I mean, if you think a year ago, five years ago, 10 years ago, the things you used to do manually that you now do digitally -- the bill paying and so on and so forth -- it's clear that all of us, whether we want it or not, are becoming increasingly dependent on the performance of the network for our daily lives. And it would be increasingly difficult for any of us to recreate some of these core daily functions manually. You know, if anything we would get on the 1-800 line and just get constantly looped around to, you know, someone named Pradesh in Bangalore to try and solve this problem, as I did an hour ago with Amex. I said how's the weather in Bangalore? He said I am in St. Louis. I said, no, you're not. You're in Bangalore. He said, it's very fine here. It's about 35C. (Laughter)

So on the one hand, we have this global dependence on the network, and yet, on the other hand, we have these vulnerabilities of the network which are frankly baked into its original design. This was, you know, the Internet as we know it now. When I was at the world famous Rand Corporation there were still, you know, very pale-skinned people in the basement who didn't go to the beach and never saw the sun very often who were there at the beginning. You know, Arpanet Node No. 3. And they would tell you that this network was never designed to have security built into it because no one who architected the network to begin with ever thought it would be used for malicious purposes. Ever.

I mean, Steve Lukasik, one of the architects of the original Arpanet, was at a Council on Foreign Relations event that I was at recently and shocked me by standing up and saying it's my fault. It's my fault. There were proposals to put security in the stack and I said no because I thought it would make the network more efficient. And, you know, I'm to blame for everything. He said -- but then he asked if there were any lawyers in the room. And he said I'm not really to blame for everything. (Laughter)

And so from the very beginning we've been sort of trying to glue security onto the side of the Internet. It's never been architected in at a fundamental level. And there's these core vulnerabilities. And unfortunately, as one of the early adopters of the Internet or the earliest adopter, we in many ways in the United States suffer from more problems than other people, such as some of the networks in China, which have been able to take advantage of the fact that they were late modernizers and, therefore, in many cases were able to go from dirt to wireless and to have much more advanced networks.

But, you know, given our dependence and given this vulnerability, I think that we still, you know, we're now racing towards this future in which we're frantically trying to basically repair the car while we're driving 70 miles an hour down the freeway. And there's an awful lot of people in industry and other places that are working very hard on this problem. But this is the world in which we all live in.

And going along with that I would argue, therefore, the threats that we face are getting more dangerous because there's so much more at stake. You know, we've gone from a world -- I mean, do you remember those halcyon days 10, 15 years ago when we were worried about web page defacements? You know, oh, they took down the web page.

You know, the Chinese hackers would hack Taiwanese web pages and, you know, put Chinese flags on them playing the national anthem. And then Taiwanese hackers would hack Chinese websites and put Hello Kitty logos on them. And, you know, the prophets of Internet cyber war were like, this is the end of the world. This is the end of the world. And everyone would go, no, its web page defacements.

But now we're looking at things like the intrusions into Google and other Silicon Valley companies that in my mind reflect a real escalation in where we are right now. And words are important. And I'll get to this in a minute. But when China origin intrusions were occurring against the Department of Defense and classified defense contractor companies, there was a part of me that said this is really serious. We really need to focus on this, but all is fair in love and war. Okay? But the attacks against Google and the other Silicon Valley companies in my mind are an escalation because those were intrusions that went literally to the heart of the American innovation economy.

And to the extent to which that data was exfiltrated and then was given to potential competitors, domestic national champions in China and other places could fundamentally alter the playing field for global trade. To me that is fundamentally different than defense-oriented espionage in the Pentagon networks, which is, frankly, just expected given the nature of the strategic relationship.

Now, if we then take it down a level and we look at China, I think in U.S.-China relations we have a fascinating China cyber dilemma because this is, in my mind, an unprecedented convergence of two things. And on the one hand, China is one of the most prominent state level cyber threats to the United States, while, at the same time, China is the supplier of nearly every information technology device that you currently have on your person and have in your home. So, you know, I've struggled to think of another historical example where the threat vector is also the supplier of all of the weapons that are basically being used against us. Or the supplier of the vulnerabilities.

And this is similar in many ways for me to the U.S.-China trade dilemma where on the one hand we have hundreds of billions of dollars of bilateral interdependent trade and yet we have these natural frictions in the strategic relationship. And for many, many years I would argue that trade relationship brought the relationship consistently back on azimuth after very serious crises.

Now, admittedly, sometimes for both sides, mainly just for the Chinese side, I always sensed a bit of a frustration aggression complex. In other words, I wish we could push our interests a little harder, but we are so reliant on this grade as the basis for economic development, which is the basis for social stability, which is the number one priority of the Chinese government. And therefore, even though our populations would probably wish us to take a stronger stance and extend this crisis, we need to bring it back on beam because the overall trade relationship is the basis of the relationship.

And for many years I would argue the business community here in the United States continued to be the strongest supporter of strategic relations with the Chinese precisely for those reasons. And therefore, to me, it's very striking in the last six months to hear American companies very quietly and now very loudly saying that they believe that they are facing an incredibly hostile environment inside of China; that they believe that whereas before it was an uneven playing field and a culture clash, that now the Chinese government in their view has reached a fulcrum point where they have just simply said we are no longer willing to be an export processing zone for your components. We wish to move to the next stage of economic development that requires indigenous innovation.

And we are going to design things like the 2006 medium- to long-range S&T plan and the indigenous innovation regulations, and the new crypto regulations to fundamentally force the transfer of innovation from Western multinational companies operating in China to their domestic counterparts, to then be pushed out of the China market and then compete with Western multinational companies globally. And I think that, you know, whether the business community is behind or ahead of the policy community in recognizing this challenge, whether -- the fact that they had to go public, which they are often loathed to do with these letters to the Chinese MOFCOM and other government entities with their concerns about this, my fear is that now this fundamental strong pillar of U.S.-China relations that has weathered all these storms in the past -- is it self-weakening? And that this does not portend well for maintaining strategic stability in the relationship.

It's interesting, though, to contrast this situation, one in which we have all of this interdependence, with that of the Cold War, where we didn't have a trade relationship with the Soviet Union, where we weren't relying on the Soviet Union for supply of critical componentry. So the crisis in many ways could get more out of hand. In the Chinese case, instead, we have this balance between threat and supplier. And I've often thought that the Chinese themselves had to walk this very thin line in terms of global -- in terms of national information security, in ways that Emily alluded to.

In other words, on the one hand, they knew they had to be jacked into the global information grid for economic development. And yet, on the other hand, they knew that these technologies they were importing, and more importantly, the methodologies and modalities that were embedded in these technologies, the values that were embedded in these technologies, the ability to use them even absent information to organize themselves across provinces, actually represented a threat to the single party rule of the Chinese communist party.

And I, too, have been incredibly impressed over the last 15 years at how well the Chinese government does. Particularly as an atavistic, backward looking bureaucracy in responding to these new dynamic technologies. I mean, the Chinese government has done a much better job of responding to these new technologies than my mother has, for instance. And then the Chinese government is more sclerotic than she is. And so, trying to understand how they became so nimble and flexible, in many ways being very observant, watching the dynamics of how these technologies are being used, then crafting regulations as sort of a "Crazy Ivan" to be able to reframe the entire economic landscape in ways that curb the development of these technologies in negative ways.

I don't think anyone at the beginning of the Internet revolution believed that governments like China and Saudi Arabia, in other words, would be so deft at handling this. Perhaps we need to look at Singapore and all of the early lessons that they taught the Chinese. All those trips that Ding Guangun took to Singapore to learn how to do this, perhaps we need to ask them.

Also at the level of state relationship, however, the Chinese, and to their part, the Russians, as well, are offering a new model not only for how to maintain a market-based economy while maintaining a surveillance state. But the Chinese and the Russians have also shown us a new model of how cyber can be an overt tool of national power in ways that I don't think the United States at a policy level is very comfortable with. I mean, if you look at patriotic hacker phenomenon in China, if you look at Estonia, if you look at Georgia, and all of those cases, it's clear to me that both Beijing and Moscow are much more comfortable with the use of cyber as an overt tool of national power than the United States is where it's still buried beneath layers and layers and layers of compartmentation and secrecy.

But not only are they more comfortable with it overtly, they're even comfortable having proxies. And in some cases, possibly even non-national proxies carrying out barely veiled attacks on their behalf that could potentially have strategic level consequences against countries with real retaliatory capabilities. And yet, feeling confident enough that the plausible deniability of the network is sufficient to shield them from the possible consequences of this behavior.

By contrast, as I said in the United States, we only entrust this kind of activity to people with lifestyle polygraphs buried deep, deep, deep in caverns underneath Fort Meade. And so I wonder sometimes about the strategic friction it causes when we have these two countries pursuing one model and the United States pursuing another. It's certainly not symmetric in the way we go about it. And I think this is a major problem we're having when we confront some of these big questions.

And what are the big questions? Well, the near term big question is what do we do about cyber espionage? And here I would argue that words matter. It's not that I disagree with Admiral McConnell or Richard Clark in all of their writings and speeches about cyber war. But we need to be very clear. And I think the Department of Defense for all of its acronymic back flips is actually -- helps us a bit in this way because they divide computer network operations into three things: Computer network defense, computer network attack, which I think many people are talking about when they talk about cyber war. And computer network exploit, which is the use of computer networks for intelligence gathering.

And I would argue that the vast majority of the evidence that has been released to the public and has been discussed is not computer network attack. It's not cyber war. It's cyber espionage. And in many -- we have seen very, very few cases of what could be called cyber war. So while Admiral McConnell and Richard Clark, you know, maybe right at the future. You know, they weren't quite as write about Y2K, but we're going to let that go. Well, while they may be right about what the future looks like. And certainly there are these structural network vulnerabilities with power grids and SCADA and, you know, all these sorts of things. So the potential vulnerabilities are there.

What we do have is a very large repository evidence of the utility of using networks for cyber espionage. And frankly, when an intelligence service looks at this issue and they say, well, we could cultivate someone for 10 years very patiently with great deal of risk and moving people in and out of countries and handlers and everything else and maybe we'll get a stack of sensitive material this high. Or maybe we'll set up, you know, a three-year extensive computer network operations, computer network exploit operation where we could literally fill this room with sensitive information documents that we've obtained, you know, at fiber optic speed. I think a lot of people are looking at that and saying, you know, the cost benefit calculus that perhaps cyber espionage is much lower risk, much lower potential of getting people caught and having to have swaps and trials and prosecutions. And given the vulnerabilities of the network, probably a much higher benefit to go at it that way.

The medium term issues are frankly all the big questions that General Alexander punted in his testimony and it's not because they're secrets. And it's not because he wants to hide the answers. Because literally nobody that I know in the system has good ideas about how do you deter in cyberspace? How do you compel? How do you do escalation control? How do you do war termination? All of the fundamental Tom Schelling issues. I mean, you can literally go through Schelling and Khan and Wohlstetter and even Ellsberg, and try and apply the template from the nuclear warfare field onto cyber and it's very, very difficult.

The fundamental problem at the heart of it is the attribution problem. If you don't know who's attacking you with any degree of confidence, then it's very difficult to deter. And if you don't know who's attacking you, then it's very difficult to develop proportional response. It's very difficult to develop, you know, displays that have value. The whole -- basically not knowing who's attacking you undermines all of the core pillars of the strategic canon that we spent 60 years developing during the Cold War. I feel like with cyber we're at

1946, you know, and where is Bernard Brody? Where is Bernard Brody's book on atomic warfare? Because that's where we are right now. And yet we're in the middle of the conflict. In other words, it's almost as if we have arsenals of nuclear weapons, but no one has developed any doctrinal materials on how to use them.

The other medium term issue that a lot of people are thinking about was, well, given all of that and given the potential threat, is there a role for multilateral arms control? And the Chinese and the Russians have been very vocal about this. And it doesn't surprise me because currently because of the attribution problem it's impossible to develop verification regimes. So everyone can sign up for a lot of feel good multilateral arms control treaties on cyber and then violate them with complete disregard from the very first day and it would be almost impossible under the current system -- if you look -- if you read the annexes on the New START Treaty and then think about how you would build a similar verification regime for cyber, it's daunting if not impossible. And so I think there's going to be a lot of pushes to develop multilateral arms control solutions. But I would just start asking the hard questions about how are you actually going to prove it other than sort of a feel good U.N. measure.

Now, of course, there is room for dialogue. And Jim Lewis is in the room and he is leading an important Track 1.5 on this, as are other people. And I think there's real value in that. But it's important to notice the things that we can talk about and things we can't. You know, we have to start slowly. We have to talk about terminology because if we're not even using the same language to describe the problem, then it's very difficult for us to have a discussion.

And we can talk about things that are not, you know, both sides don't regard as threatening, like cybercrime. You know, who supports crime other than the North Koreans, right? We can't obviously have a cybercrime discussion with them because they say we support crime.  But other countries would actually come out officially and say that they're against crime.  And so, you know, whether we can talk them into the Council on Europe Conventions or whatnot, but we have to be willing to cooperate.

A Chinese government official with the Ministry of Public Security told me recently that they had made eight requests at the LEGAT office in Beijing of things that they wanted to deal with, things like child porn.  I mean, nothing political where we would disagree about the definition of who's a criminal.  And they got no response whatsoever from our LEGAT in Beijing.  We can't go to the Chinese and say you need to be more helpful with us on cyber issues if we're not even going to be willing to respond on those issues.  I mean, some people say to me, though, we demarche the Chinese about cyber.  Why doesn't that work?  Isn't China a shame culture?  And I say, well, yes, they are, but with plausible deniability there's no reason to feel shame.

Finally, the long term issues that we need to deal with.  These are long term structural issues.  They go right to the heart of where we might be 20 years from now in this relationship.  In other words, we have to do the hard slogging policy work now to shape the Internet of the future that we want where security is better built in and we can better answer some of these questions.  Things like supply chain.  If China is supplying most, if not all of the information technologies, we're going to have to spend a lot more money on hardware and code auditing in the past than we did before simply because we have to operate now as if there is compromised hardware and software inside our networks.  We can't shut the networks off and go through them with a nit comb looking for Trojans and backdoors anymore.  We have to continue to perform the mission knowing that there is compromised equipment in the system.  That's a fundamental mindset change for people.

The Committee for Foreign Investment in the United States.  Eventually, the Chinese are successfully going to acquire companies in the United States.  Quaway 3Com was a big disaster. I mean, the entire U.S. Government went into a paroxysm. You know, if there was a Chinese trade official here I'd say, look, have Haier buy Maytag. You know, something completely nonthreatening. Get the American public used to the idea that China is going to be buying American assets.

Ownership of infrastructure. Global Internet governance. The Chinese are really trying in many ways to move global Internet governance from IKAN to the ITU because they feel that they'll have more advantages there, that IKAN is more of a U.S.-dominated institution. I don't think it's in our interest to allow that to happen.

And then finally and fundamentally, the very global IT standards that we use, the fundamental plumbing of the Internet. The Chinese are much more active and have much more focused government policies and much more attendance at the IEEE and ISO meetings on these issues, whereas we in the U.S. Government, we rely on industry reps to go defend our interests. And it's time that we actually had a serious policy and actually had a coordinated policy to be able to design the future of the Internet rather than hoping, as it did in the past, that it would simply design itself.

Thank you very much. (Applause)

MR. LIEBERTHAL: Thank you. Excuse me. Thank you both very much.

As you can see, our two speakers came at this in two different dimensions of the cyber issue with Emily focused more on the state-society relationship in China and the goal of the Internet in that and James more on the security dimensions of it.

I'd like to kick off with one question for each of our speakers and then open it up to the audience. Why don't I begin with you, James, just to pick up on your remarks.

You commented that most of what is broadly called cyber attacks or that kind of thing is, in fact, cyber espionage. It's exploitation to gain information advantage. If you look at what we know in the public domain, Chinese-based entities have acquired in terms of information that has security relevance to it, it is -- I think it's fair to say it's mindboggling. This is terabytes of information on all kinds of sensitive issues.

My question to you is I know in the U.S. system from my own limited experience there, it's one thing to gather a huge amount of information; it's another thing to sort through it to gain what is really important to know. It's still another step to package that in ways that's useful to policymakers. And it's a final high hurdle to get it to them in a form that they will actually absorb and act on. So there are a lot of steps between sucking up the information and making it useful for policy terms. Everything we know about the Chinese system and its other dimensions suggests they would be rather bad at this. You know, it's highly stovepiped, lots of competition, information doesn't flow freely, lots of disconnects between different levels of the system and so forth. Do you -- do we have any notion at all of whether the Chinese are able reasonably well to exploit the information that they suck up in such large quantities? Or can we sleep easier at night?

MR. MULVENON: Well, let me just say as an intelligence officer I always want more data rather than less. So, you know, what you're describing to me is a process problem, not an intelligence gap.

And I think you're right to point out that the conventional wisdom about China that somehow it's a monolith that there's some guy stroking a white Persian cat in his lap in his floating volcano island headquarters. When you actually rip open policy issues as you have in your writings, you realize that it's often more internecine, more bloody, more partisan, if only because the org chart is really the opening bargaining position as to who actually has authority, whereas the informal power matrix is also important.

What has struck me if you look at Chinese espionage -- and I'm actually writing a book right now called Beyond Espionage that looks at Chinese espionage in a much broader frame. It looks at, you know, the transnational brain drains. It looks at, you know, students. It looks at technology flows. It looks at foreign RD labs in China. What we found in many of -- for instance, the technology espionage cases that have both cyber and physical dimensions that in fact we found very few professionals as I would call them engaged in the espionage. But instead they were sending scientists and technicians and engineers from the exactly appropriately relevant numbered institute for that particular technology to come over and negotiate its either illegal or legal acquisition. In other words, the technology was then being fed back to precisely the people who know what to do with a traveling wave tube or people who would know what to do with this piece of code or something along -- this analog to digital converter.

On the cyber side as well, what we see when we look in their technical writings and even when we look into their internal writings about illegal technology acquisition is this very strict adherence to this idea that you need to mobilize the subject matter expert population first -- the numbered institutes, the universities that have government affiliations, and have them involved from the beginning so that you know exactly what you want to get.

Now, there is this other category of military intelligence information about how is the NIPRNet structure and how does Pacific Command do logistics. And I would think that that kind of information would also be recognizable to people in their logistics community who would understand, you know, the movement of material. It can be handled that way. So while I'm not saying that there's this thousand grains of sand sifter -- and I've always hated that analogy because I don't think it represents all of the dissent and clash and competition within China -- what I've been struck by is the extent to which very, very obscure technologies are being acquired and being analyzed by people who actually know what they're looking at.

MR. LIEBERTHAL: I guess I should go out and get Ambient.

MR. MULVENON: Tylenol PM.

MR. LIEBERTHAL: Thank you.

Emily, you took your broad topic of the Internet and society in China and focused on essentially providing organizational tools to those who want to make changes in China. And framed it in terms of we've gotten a lot more sober, if you will, about the capacity of the government to use the Internet to maintain harmonious society. Let me ask about a different dimension of this because to me -- maybe it's because I first went to China in the mid-1970s. It was a very, very different world then. And to me one of the most dramatic changes in China is that people in society interact regardless of their work unit. You know, it's now open in communications on other than organizing around political issues.

I guess my question is do you get, I mean, is your -- you focus on the Internet quite a bit. Is the Internet really contributing in a major way to Chinese society feeling like a serious part of the polity in China? In other words, most people aren't concerned with overthrowing the government. But how dynamic, how much tinsel strength is there to Chinese society as versus, you know, 25 years ago when the state effectively locked people into work units, limited their communication so they were within those work units, and made them utterly dependent on the work unit for their prospects? This is a very different world now. How critical is the Internet in sustaining and nurturing that different world?

MS. PARKER: In terms of affecting the policy -- the overall policy?

MR. LIEBERTHAL: No. In terms of whether society is really something to contend -- in other words, does society have its own -- is civil society forming? Not necessarily around changing the political system, but forming around all the issues that most people care about most of the time.

MR. MULVENON: And creating social solidarity.

MR. LIEBERTHAL: Thank you. I was obviously wrestling to find the term, so thank you.

MS. PARKER: I think that's a key question. I think the answer is yes. I think there's sort of two aspects of this. I think you're absolutely right in that the majority of Internet users in China are not using it for political reasons. I mean, most people in China are, you know, playing online games or talking about their cats. I mean, the same as here in the U.S. I mean, most people using the Internet here are not, you know, have any sort of broad political cause.

However, I think that even in those people, if you ask the average Chinese netizen -- and when I say "Chinese netizen," I mean the average -- the person who's just like doing online gaming or whatever -- they're not going to talk to you about abstract concepts like freedom and democracy. But I think, you know, we're dealing with a very different generation in China. I mean, you're dealing with like the post-80s. You know, people like who are really used to a totally different level of economic development than that of their parents, and they're used to getting what they want, and they're used to getting what they want quickly. And I think people like that will actually end up pushing change in China in a very different way.

I mean, you know, there was, for example, in Beijing, you know, they tried to regulate the size of dogs, you know, for a while. Do you know what I'm talking about? There was this thing where they tried to say your dog can only be this big or, you know, they wanted to have like a dog rule. And basically all these young women just completely got upset about it and they, you know, they started fighting back. And I think, you know, these aren't overtly political issues, but I think you're going to see a lot of these people who seem apolitical gathering in order to, you know, push for change. And the Internet is one tool that's allowing them to do that, even if it doesn't look political like immediately.

The other thing though is that one of the things that I didn't get to talk about is how the Internet is affecting the state media. I think that's an important thing. I mean, if you go to China and you talk to people, you'll realize that officials are really monitoring what's happening on the Internet in terms of, you know, deciding certain topics. Do you know what I mean? Because China doesn't have a public square in the sense that, you know, as we think of one here. So the Internet has become a kind of public square. So for officials to gauge reactions to policy or to issues, the Internet is one place to look.

You know, most specifically one -- I spoke to somebody from CCTV once and we were talking about the widespread opposition in China to Japan's bid for a permanent seat on the Security Council. And he was talking about his own coverage of it and he said that, you know, I actually have his comments here because I thought it was really interesting. You know, Japan had this bid. There was a Chinese Internet petition. It obtained about -- at least 22 million signatures. Some people estimate as many as 40 million signatures. And this CCTV journalist told me that public opinion, as was gauged by the Internet, may have actually played a decisive role in determining the reporting of the state media. And he said to me -- and this is what I had written down what he said -- he said, after the reactions on the Internet the government changed so we had to change. We had to report every day on how these efforts to gain a seat on the Security Council were going. Before this era, government could act unilaterally. Now, when something happens on the Internet the government has to change policy.

So this is a very interesting comment coming from somebody coming from CCTV, which is, you know, a very -- which is basically, you know, a state channel and it's very, very influential. So I think, you know, we are seeing the Internet -- in fact, you know, forming a sort of civil society in that way and that it's affecting state coverage. And because the Chinese government, as we all know, is so concerned with stability, you know, if they see a kind of unrest on the Internet -- if they're seeing petitions, if they're seeing these groups forming online -- you know, they're going to take it pretty seriously. How they're going to respond to it is not always clear, but they will take it seriously. So I think -- I don't know if that answers your question.

MR. LIEBERTHAL: Thank you. The floor is open. Please, we do have roving mics. And please say who you are and then ask your question.

Yeah, Tony.

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

I want to speak to Ms. Parker's presentation. I'd like to make a comment if I could. I'd be happy to have a response, but I don't know how to phrase it as a question.

MS. PARKER: Sure.

MR. KANE: Because your presentation reminds me a lot of the kind of talking about human rights issues in the 80s and 90s. And one of the problems I had back then was that we branded human rights as a U.S. thing. And that made it very easy for Chinese to reject because they didn't want to be seen as agents of the American government. And I hear a lot of that and you said it at the very end of your presentation about U.S. branding for the Internet. You know, like, I thought human rights was supposed to be a universal declaration. I thought cyberspace was supposed to be beyond boundaries in the same way. And I think the more we try to identify it with the United States, the more likely you are to get that kind of reaction that you said you fear where the Chinese nationalists will react against it.

And I see part of that coming from the idea that there's this frustration that it isn't turning out the way we wanted it to turn out. But for those of us who have been around a long time, I mean, the Internet -- there's no question that this has changed China. And there’s no question that it’s mostly open.

I mean, whenever I see -- you know, 20 years ago or 15 years ago there were lots of things that I knew about that my Chinese friends didn’t know about. Now I play this game. I experiment. I try to find the things that I know the Chinese government are trying to block and ask my Chinese friends do you know about it. And they immediately send me 10 websites, you know, where they learned about it. I mean, they’re very good at getting around the Great Firewall. And I think that we should be kind of empowering that kind of thing rather than lamenting that it isn’t 100 percent like we have it here and therefore we’ve somehow failed.

MR. LIEBERTHAL: Thank you. Do you either of you have a response to that?

MR. MULVENON: Well, I do think there’s an interesting backlash going on in the sense that the early cyberspace people said that this is a realm that exists independent and that this is a place in which disaffected alienated people could go that is beyond sovereignty. And I think the trend lines for the last couple of years, particularly in the coverage on Google, are to remind people that every bit of what we know as cyberspace exists in physical space as servers inside sovereign countries. That there is no independent cyberspace that exists outside of national sovereignty.

And to that extent, you know, for a long time I think that the media -- the tech media treated Google almost like this nonprofit international governmental organization that was just this universal good. Google was just a universal good. And, in fact, the French and the Germans and many countries now are saying, now wait a minute. Google is amassing enormous amounts of private data on our citizens and commercializing in ways that we’re not comfortable with, with our domestic laws. And I think that there is now, you know, as these countries begin to reclaim the Internet, it’s inevitable that we see people putting up walls and having greater censorship and greater focus on security. And ultimately, you know, even the president himself here in the United States has said if we want to have better cyberspace security we probably need to confront issues like identify and authentication, which is completely amicable to the notion that you could have this anonymous presence on the net and yet we're at this crossroads where for security reasons a lot of people are saying if we want real security we're going to have to give up some of that anonymity that we've enjoyed. Otherwise, it's just going to get worse and worse in terms of the security problems.

MR. LIEBERTHAL: Hank?

Mr. LEVINE: Hank Levine with the Albright Stonebridge Group.

On the question of the sort of computer network intrusion exploitation issue, I guess just from press reports I get the sense that over the years the U.S. Government has wrestled with this issue of whether the U.S. Government should be in the business of commercial -- collecting commercial intelligence. And my sense is that, you know, we don't particularly -- and it's a tough issue. You get the secret formula. Do you give it to Coke? Do you give it to Pepsi? Do you give it to the smaller bottler? You know, sort of how do you deal with this? And you alluded to this I think in your comments. One of the characteristics -- you also mentioned the notion of sort of trying to access classified, you know, military information. It probably falls under the category of all is fair in love and war.

It strikes me that one of the characteristics here of the Chinese effort, whether it is again directly through actions of the Chinese government or through proxies, is this very heavy emphasis on collecting commercial intelligence, commercial information, whether it's code or whatever. I was just curious, sort of broadening out the picture, to what extent -- and I understand your focus, of course, in research is mainly on China. But to what extent is this sort of common in other countries? Again, every now and then I see a press report about the French government allegedly opening briefcases of U.S. business people. And you hear other countries raised as well. So I'm just trying to get a sense of when we think about the Chinese effort here, is it the scope and how good they are at it? Or is it -- are they truly an outlier with regard to this issue as we look all around the world?

MR. LIEBERTHAL: I'm sorry, this issue being the commercial espionage?

MR. MULVENON: Yeah. The use of commercial.

MR. LEVINE: The use of commercial -- the sort of governance.

SPEAKER: Right. Right.

MR. LEVINE: Government backed efforts to collect commercial.

MR. MULVENON: Well, I would probably assert that among countries with serious intelligence services, the United States is alone in not using its intelligence services to gather information on behalf of its private sector companies. And that is clearly not true in a number of cases. And there's a reason why the Israelis and the French and the Russians and the Chinese are all usually mentioned in the same breath. And it's because both, whether it's physical or technical espionage that's been going on for a long time. I think what's animated people at the China case is the scale and the brazenness of it. And they also have been involved in some fairly high profile intrusions that were particularly damaging -- precisely at a time when the national policy apparatus is directly confronting this issue and we have a presidential comprehensive national cyber security initiative, spending anywhere between $18 to $31 billion dollars on cyber security. And we have the stand up of cybercom and all these other things.

And so when people are grasping around for the relevant examples of why we need to spend all this national blood and treasure, why we need to have these big reorders? And why does it need a fourth star and all these sorts of things. Those are the national examples that they're grabbing. It's not to say that the Russians and the Israelis and the French aren't also engaged in this heavily. Not to mention, East European criminal gangs and other people who are, you know, assembling gigantic botnets and credit card schemes and everything else. So, I think the Chinese are victims of bad publicity, but it strikes me the extent to which the bad publicity hasn't abated it whatsoever. I will say, you know, obviously my corporate networks and me personally have been a consistent victim of a lot of these intrusions. And I haven't seen them abate in the slightest even being on the cover of Time Magazine.

MR. LIEBERTHAL: Bobby?

MR. O'BRIEN: Bobby O'Brien with Brookings. I have a question for you, Emily.

MR. LIEBERTHAL: Go ahead.

MR. O'BRIEN: I arrived in China at the end of the Olympics in 2008. At the time YouTube was accessible, Facebook was accessible, numerous blogs were accessible. Over the course of the year those were sort of all taken away. And at the time it was attributed to a series of anniversaries. But when these anniversaries happened, security was tightened across the city; public squares were shut down and so on and so forth. But the restrictions were always loosened at the end of the anniversaries. These blogs, YouTube, Facebook never came back. After the Shinja rise, you had the Chinese government begin a war on proxies. And I'm kind of wondering what was the policy push behind all of that? Why did they all of a sudden decide to make these restrictions permanent as opposed to do it temporarily during the sensitive period?

MS. PARKER: I think that's a really good question. I mean, I think, you know, there's -- a lot of it is guesswork, but I think, you know, there's a few potential reasons. I mean, I think -- the events in Iran I think probably really scared -- were frightening. I think China watched Iran very, very, very carefully, both the government and the people. And I think, you know, there’s some controversy about the role that something like Twitter or YouTube played in Iran. But I think we do know that it did play some role. How big a role we don’t know, but YouTube in terms of like sending around, you know, cell phone videos; Twitter in terms of letting people organize. So I think that that’s a factor that again I can’t say for sure, but I’m sure that -- I personally believe that they were probably watching Iran.

I think also, you know, again, if you go to China now, and I’m sure many people here go frequently, you know, China -- we tend to look at China as, you know, booming China, you know, America’s banker and, you know, all this. But if you go to China you can sense a certain degree of nervousness there. Nervousness about all sorts of things. Nervousness maybe about housing prices. Nervousness about ethnic unrest. And I think there’s generally a sense that the party is nervous about something and that nervousness seems to be increasing. And I think, again, as long as they feel some sort of uncertainty about stability, we’re going to see these sites blocked.

You know, another thing that I think is extremely important to keep in mind is that one of the reasons that they don’t like Twitter is because it’s seen as a way to spread rumors or to spread false information or to ignite passion. And the problem is that in China it’s unclear like what the -- what media you can trust in China. Like, you don’t really know. And until there’s a sense that, like, okay, here’s the actual story. Here’s actually what’s going on. I think these sort of rumor-spreading devices will have a lot more power -- will have outside power. Do you see what I’m saying?

Like, I think here it would be hard for Twitter in the U.S. to spread like a completely baseless rumor and just ignite the masses to do something. In China I think it would be easier because there’s less sort of, you know, there’s less trusted sources of news.

MR. LIEBERTHAL: I’m sorry. There’s a side conversation here. FOX News does that. Forgive our political thing here.

Let's see. Back there. Not way back, but back last row of seats. Yeah, right there.

SPEAKER: There's been a lot of focus in the discussion on the Internet as a tool for dissidents as a tool for rebellion. But not as a tool for incorporating Chinese people into the system and for political participation as a sort of collaborative or discursive democracy.

I think of recently in November 2009 the Ministry of Commerce and the NDRC posted on their website an open call for comment on trading or opening A-shares to foreigners. And recently, legislation passed to that effect. Could you comment on how much influence you see on this phenomenon of collaborative or discursive democracy and political participation through the Internet having on China?

MR. LIEBERTHAL: Let me add to that as you frame your answer. Local governments all over China now post kinds of information that in the past we would have died for.

SPEAKER: Right.

MR. LIEBERTHAL: And open it up to comment. So just as you --

MR. MULVENON: Am I to say thank you to the Chinese government at all levels for posting large amounts of information on its websites because it's a fundamental part of my business model and I'm renovating my kitchen. Thank you very much. (Laughter)

But more to your point, I think that, you know, Shanthi Kalathil and Taylor Boas a number of years ago wrote I thought a very interesting monograph here in D.C. that talked about, you know, oh, yeah, I realize it's all doom and gloom. You have the human righters on one side and then the securocrats like me on the other. And isn't there some middle ground where the Internet has a positive effect upon the development of civil society and as a channel for articulation of public preferences inside a system that is nondemocratic?

And there are many, many, many examples I would argue where the government and the party in particular have used the Internet in ways as Emily said as a way of plumbing public opinion. I mean, go to Beijing now and buy books on Mishu Gongzuo, on secretary work. Being a secretary to a senior leader. There's entire chapters on how to use technology, how to use blogs, how to use the Internet as ways to help your principal better understand the feelings of your constituents. This is now absolutely de rigueur now if you're going to be an assistant to a senior leader. You're going to be his blog person. I mean, somebody told me that there's actually a unit in the foreign ministry -- god help these guys -- that do nothing all day, but sit in international affairs-related blogs and monitor what the blogging population is upset about, just so that they can write a daily memo for the minister so he's not surprised when there's this dramatic upswing -- upswell among greater China about this or that incident involving the Japanese or the Indonesians or the Indians or something like that, whereas in the past they were surprised by it.

And then you see an enormous amount of E-government stuff. A similar example to yours was the one in which the Beijing municipal government wanted to have a toll road. And so they had a six month comment period on the Internet about how much they should charge in tolls, which was then followed by a series of open public meetings about how they should -- and ultimately the dollar amount that they charged on that toll road was the median point of the discussion on the Internet.

And I think this really gets to this issue -- I mean, I know people like to make fun of Jiang Zemin and the theory of the Three Represents. But I always thought it was incredibly serious because, you know, all of the jargon aside it was really a recognition that the party needed to find ways to bring all of these new social forces created by modernization into the political conversation in China and understand what their preferences were because as these new aspects of modernizing societies became more powerful, if they were outside the candy store with their chocolate smeared mouth pressed up against the glass they might get angry to know that they couldn't get involved in choosing what kind of candy was available in the store.

And so I think these are all very important. But the problem is the very technologies and the very modalities that facilitate that kind of E-government are the same kinds of channels that potentially allow for anti-government behavior. And that's the great balancing act that I referred to earlier.

MS. PARKER: Quickly to add to that, yeah, I think that's a really good question. You know, I don't mean to overly emphasize the dissident question because I actually don't think it's dissidents per se that are going to be driving change in China. Rather, it sort of the ordinary citizens who want information because they feel that some injustice has been done to them in their daily life. You know, it could be something about local corruption. It could be something that they feel that that's going to be driving people. A sense that they want more access to information just to improve the quality of life. And that's -- a lot of the movements, you know, that James is alluding to are started by people like that, not necessarily people who again are fighting for, you know, democracy or overthrowing the government.

MR. MULVENON: Yeah, things like Nail House. I mean, that's a perfect example of the use of the Internet to illuminate the problem of a local economic issue. You know.

MS. PARKER: Exactly. And the other thing to keep in mind is that, you know, some of the most powerful forces on the Internet are not necessarily forces for reform. I mean, for example, what we think of as nationalism, Chinese nationalism, I mean, that's something that the Internet is a breeding ground for that. And I think that's actually scared the government for other reasons, not because they were trying to, you know, insight some sort of overthrow, but because it was more nationalistic than the actual official line.

You know, we've seen, for example, with Japan, we've seen some very, very strong anti-Japanese movements on the Internet that the government has actually shut down. You know, and so I think, like, again, there's all these different things and it's easy to simplify this and say, oh, the Internet is a force for good and a force for reform in China. I'm not necessarily saying that. I'm just saying that it will shake things up basically. And it is a threat to some degree to some sort of like one monolithic wall of information. But it doesn't mean that everything that's happening on the Internet is a force for democracy because it's not.

MR. LIEBERTHAL: Yes, sir.

MR. McREYNOLDS: My question is --

MR. LIEBERTHAL: The microphone is coming right to you.

MR. McREYNOLDS: Thank you. My question is probably for James --

MR. LIEBERTHAL: Excuse me. Who are you first?

MR. McREYNOLDS: Oh, I'm sorry. My name is Joe McReynolds, and I'm a graduate of Georgetown SSP.

And I'm wondering about the rise of voiceover Internet and video technologies for communication in China. I spent the last year living in a couple of different cities in China and all of the tech-savvy 20-somethings I talked to were very excited about the rise in bandwidth, rise in video and voice communication over the Internet. And I'm wondering how that raises the costs of maintaining real control over discussions through the Great Firewall. I'm wondering if at a policy level Chinese policymakers have essentially given up on really trying to reign in discussions in any meaningful way and just really blocking the offending sites, but taking a more laissez-faire approach to say trying to figure out -- unless you're one of the top 100, top 200 activists -- trying to figure out what you're talking about over voice communication, video communication, things like that.

MR. MULVENON: Well, again, the Chinese were -- the Chinese government and the security apparatus were on this pretty early. I remember talking to Baltong Sun who said that he was communicating with his father via voiceover Internet protocol early on and that they eventually started hearing other Chinese voices on the line of securities guys, you know, changing shifts listening in on their VOIP. And I know that, you know, all you have to do is go back and look at the Skype controversy from a couple of years ago about TOM.com and realizing that, you know, all of this Skype traffic that TOM was running was being siphoned off and analyzed on servers that were run by the Ministry of Public Security.

And so that I think is a direct reaction to the fact that, I mean, almost everybody I know in China communicates via Skype and via other ways, not only because it's cheap -- it's much cheaper than international phone lines. And there are a whole -- there's a whole layer of surveillance technologies that Keith Bradsher in The New York Times and other people have written about that have been imported into China that allow people to monitor large amounts of this traffic. And so right now my research -- my personal research is focusing a lot on this balance in the surveillance society.

I mean, you know, what's funny, though, even the official media, when they talk about this stuff, are somewhat breathless. China Daily, which used to be the most incredibly boring publication in the world, when I was in Beijing in November there were nine straight pages of scandals and lurid corruption stories and murder and, you know, and everything else. Like, is this China Daily? And then in the back there was this tiny little article that says, you know, Chongqing municipality has surpassed 500,000 CCTV cameras, you know, meetings its 2010 goal for surveillance, you know, which is part of the nationwide network of 17 million CCTV cameras.

And so thinking about, you know, that kind of a world -- now the important thing is, is everybody looking at every screen at every moment? No, of course not. But it's the panopticon. You never know whether anybody is looking at your telescreen at any given moment. So, if you believe that the system is ruthless in its suppression, if you were doing something wrong you have to act as if someone is looking through that telescreen. Right? And that creates this self-censorship, self-deterrence phenomenon that to me is much more powerful than 20,000 Jingjing and Chachas or 50,000 Jingjing and Chachas staring at you on, you know, with their little cartoon icons on the computer screen.

MR. LIEBERTHAL: Ching Ching and Chachas, Jing Cha?

MR. MULVENON: No, it's -- Jingjing and Chacha are the little male and female cartoon police characters that randomly appear on your computer screen to say, you know, we might be monitoring your traffic. And they appear at the bottom of web pages to say this page is certified by the Ministry of Public Security as having met these information security guidelines. They're very -- they're adorable, Ken. (Laughter)

MR. LIEBERTHAL: I was in China last week. I didn't run into that. I use a, you know, VPN.

MR. MULVENON: Yeah.

MR. LIEBERTHAL: And I went from one hotel to another. And the second hotel, literally every 10 minutes I got kicked out of my VP and I had to log back on. And I assume that was a little game hoping I get tired of it and I'd just keep on working without being on the VPN.

MR. MULVENON: Well, the reason VPN works is because it uses exactly the same encryption technology as your credit card purchases on Amazon. So if they were to block those ports and those protocols, they would basically destroy E-commerce in China. And no one will do that.

MR. LIEBERTHAL: Good stuff. Yes, ma'am.

MS. WELCH: Kate Welch, CNA China Studies. Looking back it was just about a year ago that there was the Green Dam episode in China. And I'm wondering to either speaker, what do you think are the lessons learned for China domestically in making changes to the way that they govern the Internet and the international community in the way that they deal with China?

MR. MULVENON: I think that the lesson learned from Green Dam is don't publicize that you're putting spyware on everyone's computer because if you publicize it then you're going to cause a groundswell of people who don't like that. The better way to do it is to, you know, I mean, if you have a pirated copy of Windows in China, there is spyware and viruses that come onto your computer that will update your pirated version of Windows in exchange for loading adware and spyware onto your computer. It's sort of this horrible bargain you have to make in China if you're unwilling to actually pay for a bonded copy of Microsoft products.

And so better not to be on the client machines; better to still have better technology at the Internet service provider level. Better to have better technology at the national IP level. And companies like Quaway and other people are doing a really good job of upgrading those technology networks. I mean, really the Beijing Olympics, as someone mentioned earlier, was really in my view sort of a laboratory microcosm of what China is going towards in terms of a vision for a national surveillance society. And you saw it on a small intense scale around Beijing. But none of that surveillance apparatus that was assembled for the Beijing Olympics has gone away. It's just, you know, some, you know, in the past Montreal in '76 they would say, well, if we host the Olympics we'll have all these wonderful soccer stadiums. But in Beijing by contrast, all the sports facilities are empty, but now they have this wonderful surveillance apparatus.

MR. LIEBERTHAL: Yes. Can we get a mic over here?

MR. NITSKU: Yannis Nitsku with the E.U. Delegation.

I would like to ask about James' point that the trade relationship between China and the U.S. is really at the core of the relationship. And having said that, to what extent would you say that the current debate about Internet freedom might threaten or jeopardize the entire economic or trade relationship?

And also, about the economic aspect of the Internet freedom debate. How do you feel about some -- about the mounting pressure towards the U.S. Government from Google and other companies that the U.S. Government should bring a case against China to the WGO saying -- arguing that Internet censorship is sort of a barrier to trade? And how do you think might China react to such an action? Thank you.

MR. MULVENON: Well, I think the second half of the question is easier to answer because I think the U.S. Government would be very loathe to go down that road of saying that Internet censorship was a barrier to trade because it would be too easy in many ways for the Chinese and for other governments to instead turn around and talk about PATRIOT Act and CALEA legal restrictions in the United States. I mean, all you have to do is go to Cryptome.org and various leakers have now revealed the monitoring manuals of every major telecommunications and Internet service provider in the United States, whether it's Cox or Verizon or AT&T. In order to, you know, comply with federal wiretapping. And in fact, Google itself is cautious about raising this issue because what surfaced during the Google-China episode was that the Chinese had gotten into their federal compliance wiretapping system. And so they don't really want a lot of publicity about that because they're asking us to trust us to put our data up in their cloud and they can't even protect the federal wiretapping system that they built.

The first half of your question, I don't see a direct linkage between Internet freedom and the trade dispute. I think that both in Europe, frankly, and what the European business associations and trade associations have said in concert with their American counterparts is that there's even deeper, deep muscle structural issues in the trade relationship that have gone ignored for too long. I mean, everybody knew that the market was tilted in ways that benefitted Chinese companies, particularly ones that had spun out of parent ministries and those ministries were then the regulators of those companies. And this was just the nature of an uneven playing field in China. And that was fine. That was just the cost of doing business in China.

But this new series of regulations about -- that were designed to transfer innovation, I think get at the heart of the idea that, you know, that they don't want to partner with Western companies. They really want to extract information from Western companies so that they can go to this next stage of economic development. And I think at that point it fundamentally threatens the core intellectual property of all of these companies that have been investing in China, thinking that they were partnering with Chinese economic growth, only to find out that they now were seen as simply a source of food for Chinese economic growth. And that has led to -- and I was very disappointed at a policy level that we once again pronounced that our top trade priority in the strategic and economic dialogue was going to be the currency issue, when in fact people who look at the trade issue said that, you know, really the structural issues we need to talk about are the indigenous innovation regulations and other things.

MR. LIEBERTHAL: I actually think those will come up also come up also.

MR. MULVENON: Right. In terms of the main talking point.

MR. LIEBERTHAL: Right. Thanks. Back here. We have time for two more questions if they're both very brief. And I'm going to take both questions and then ask for whatever comments you want to make in response. We've only got three minutes left. Please.

MR. TAYLOR: Okay. I'll be quick.

Rick Taylor, DOD.

My question is about cyber threat and cyber espionage. One of the key pillars would be not to show your cyber capabilities, and I think the U.S. is doing that pretty well.

Now, some countries have. We're looking at, you know, Israel did, and Syria, Russia, Georgia, Estonia to that effect. Chinese have, but to me it almost seems as if it's sloppy. I don't know if it's to see how we'll defend or whether it's just that they're still up and coming with a ragtag approach. And my question is, is it a bad thing that the U.S. truly hasn't shown their cards in both the near and long term?

MR. LIEBERTHAL: Thank you. And final question? I saw a hand over here just a second. Yeah.

MR. LIU: Lawrence Liu, senior counsel at the Congressional Executive Commission on China.

Just a short question. Do you think that U.S. policymakers, mainly, you know, members of Congress and the Administration, do you think they have a coherent strategy in terms of dealing with China's censorship of the Internet? If not, what would be your recommendation for how -- maybe in terms of how much money should be spent -- where that money should be targeted in terms of, you know, promoting (inaudible).

MR. LIEBERTHAL: He thinks it ought to be spent on his company. But anyway, please.

MR. MULVENON: Well, I would -- in answer to the first question, it's difficult because you say, you know, think about the pillars of deterrence. There is a widespread belief among Chinese government, Chinese military analysts, and the Chinese population that, in fact, the U.S. has overwhelming asymmetric advantage in computer network attack capabilities that we are ubiquitously intruding their networks currently. And you read this just chapter and verse -- internal materials, external materials -- so you would think that that would be sufficient to create a deterrence regime in which our capabilities had credibility.

The problem is what doesn't have credibility is our willingness to use them. And so, you know, there have been a number of stories recently where we've talked about successful uses of cyber attack capabilities. But we're sort of tripping over ourselves. I mean, a case in point was the discussion about the Yemeni jihad websites and the debate about whether we should take them down or leave them up. You know, as an intelligence officer, I never want to allow someone's computer network attack operation to screw up my computer network exploit operation. I always want the command and control networks to be up so I'm listening, rather than having them down so they have to go to different channels.

But I think that the bottom-line is that we have a real deterrence asymmetry problem with the Chinese because of our inability to actually attribute behavior in ways that allows us to then develop a whole regime of responses that are credible. And that's why I actually advocate moving away from attribution and towards this notion that Jay Healey and Greg Rattray and others have put forward called responsibility. In other words, if it quacks like a duck and walks like a duck it must be a duck. And at a certain level nation states are increasingly held to task for hostile packets emitting from their country, whether it represents state directed computer network attack or not. And therefore, we can then grade it greater confidence that if a hostile packet is emitting from China it must at least have state sanction and sort of changing our whole mindset about how to think about that.

MR. LIEBERTHAL: Emily, do you have anything?

MS. PARKER: Yeah. Just in response to the last question. I think that the current -- I think that the State Department does actually understand the importance of, you know, technological diplomacy. I think it's, you know, there are some exciting things going on. I mean, it's sort of what they refer to as 21st century statecraft. And, you know, I think they are -- they do understand the role of companies like Twitter in promoting change in China. But as I said earlier, I think there's a lot that can be done by private companies. And I think that's sort of where we're at now where we're sort of looking at like how private companies can also take a lead because the benefit to doing that is that they are not -- they are somewhat apolitical. And so I think that's something that, you know, is sort of the next step in this -- for this problem.

MR. LIEBERTHAL: In wrapping up, several things. One, I want to thank Richard Bush and CNAPS for partnering with the Thornton China Center to put on this program today. We've heard mention today of the various dimensions of this issue: mischief, defacing websites, that kind of thing, cybercrime, issues of privacy and political freedom, issues of commercial competitiveness and innovation. And what's been mentioned in passing, but not accord very much, disabling security attacks via cyber capabilities. This is just a huge set of issues. I believe within two issues this will be central to the issues in U.S.-China relations as you begin to see these things surface.

So I really want to express our joint appreciation in all of us to Emily Parker and James Mulvenon for coming by this afternoon and helping us to begin to explore this very important set of issues.

MS. PARKER: Thank you.

MR. LIEBERTHAL: Please join me.

* * * * *

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.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012