

*East-West Center/US Asia Pacific Council
7th Annual Washington Conference*

U.S.-Asia Pacific Relations: Transitions In a New Era

May 6, 2010

“Democracy, Activism, and Information Flows”

Moderator:

Dr. Kenneth Lieberthal, Director, John L. Thornton China Center, The Brookings Institution

Speakers:

Ms. Audra Ang, International Nieman Fellow, Harvard University and Correspondent, The Associated Press (China)

Dr. James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies

Dr. Irene S. Wu, Director of Research, International Bureau, Federal Communications Commission

LIEBERTHAL: This panel takes up a subject that is of rapidly growing importance. That is the digital transmission of information, which affects everything from the nature of political organization to human rights, personal privacy, commercial security, and national security.

I am delighted this afternoon to have a panel that will explore substantial chunks of that broad continuum. Our first speaker is Audra Ang. She is an International Nieman Fellow, currently at Harvard University as well as a correspondent with the Associated Press, based in China.

The two broad issues I've asked her to address are (1) the role of the Internet and new media in her own reporting about dissidents and other sensitive topics and (2) how the availability of the Internet and other new media affects strategies pursued by those dissidents and the ability of people to learn about sensitive topics. Her remarks are on background and should not be cited anywhere.

ANG: As Ken said, I was a general news reporter for the AP in Beijing for seven years. In my reporting, I had

to not only find the news and make sure that I covered it in an objective way, but also protect the safety of the people I interviewed.

So what I'm going to do is give you a simple overview of the Internet in China, how the government censors things, and how citizens are reacting.

This information is compiled from research done by people far more knowledgeable about the subject that I am.

[Audra Ang's Power Point presentation is available at http://www.eastwestcenter.org/fileadmin/resources/washington/usapc/uap_panel.ppt]

At the end of 2009, there were 384 million Internet users in China. It's probably up to 400 million by now. The top three uses are online music, online news, and search engines. In terms of age groups, Internet use is dominated by students in the ten to 19 year range.

China has one of the largest and most sophisticated filtering systems in the world and it has gone to great lengths to limit access to any content that might be potentially critical of the government or undermine the state's control of social stability.

One example is the Green Dam Youth Escort, which China tried to put in place last year. Beijing wanted Web filtering software to be installed into every new PC shipped into China. The excuse was that the government



Ms. Audra Ang, International Nieman Fellow, Harvard University, and Correspondent, The Associated Press (China)

continued on page two

continued from page one

was trying to block children from accessing porn, but in reality it blocked a lot more content. There was a great deal of protest and eventually this software was shelved.

Some of the basic methods that the government uses to control what people see on the Internet includes filtering, in which the network administrator blocks access to specified Web pages. The administrator monitors domain names, Internet addresses, and so forth, with an eye toward specific keywords or phrases.

Methods of Censorship

The second method is the deletion and removal of content. We had to deal with this a lot because we starting to look at blogs, chat rooms, and other new media to look for potential stories. What would happen is that we would find something potentially newsworthy, but then within an hour would be gone. So I started to do screenshots or print out what we found so that even if I had to look at it a few hours later to write a story, I'd have a record of it.

Another censorship method involves deploying people to track online activity. They monitor what goes on in cyber-cafes or enter chat rooms and blogs just to keep track of what's happening.

In addition, the government has been using cyber-attacks in an effort to control what appears on the

In this environment, it is easy to become psychologically affected and begin to self-censor your Internet use

Internet. Many of these attacks have been on sites run by human rights activists. Basically, they flood the site and overwhelm the servers and rendering the sites inaccessible.

Similarly, the government has begun to hack into the email accounts of human rights activists, exiles, dissidents, and now journalists and academics. That has two consequences: first, those affected are left without email accounts, which is one of the main ways they communicate; and second, their sources may be endangered.

The Chinese government has begun hiring people to write favorable comments about the government in blogs and social networking sites. These people have been derisively called the 50-Cent Party, because a lot of them get paid to do this. A Hong Kong researcher last year determined that the government is paying about 280,000 people to do this. In addition, there are volunteers, like retired party members or college students who are part of the Communist Youth League, who are posting these favorable comments in blogs.

Finally, I would say that when you are in this environment it is easy to become psychologically affected. So Internet users become worried about getting caught or being penalized for what they're doing and so they start self-censoring.

Type of Blocked Content

What's blocked? I think all of you know this. The basic things like Twitter, YouTube, Facebook, and blogs. Search engines also are controlled for topics like Tibet, Falun Gong, Charter 08, and so forth.

In the past few years, the hot word has become *fan qiang*, which loosely translates to scaling the Great Firewall. There are several ways that Chinese Internet users have begun doing this. Some people, such as myself, have begun to use proxy servers, which link your computer to an overseas server so that you can get access to whatever you want to look at.

When I went home to use my computer, which was linked to a local server, I had to use a proxy called Hotspot just to access Facebook.

There also are anonymity networks, Tor being one of them. It bounces communications around the world, so that people can't really pin down your location or pin down exactly what you're looking at.

Another response has been informal gatherings of bloggers and journalists, where they teach each other how to use these circumnavigation tools. We are beginning to see more and more people exchanging knowledge and of ideas about how get around government censorship as they become more discontented.

As I said earlier, there's also a group of people that have begun to download articles, photos, and videos on potentially sensitive subjects in case the government takes them off the Internet. They later repost this subject matter on other sites or they send it to their friends via e-mail and other social networks.

And then there are now loosely organized groups, who research China's censorship mechanisms and they uncover companies and organizations that help build the the government's censorship system.

Word Plays to Beat Censors

Last of all, people are beginning to protest in a more fun way by playing on words. And I'm going to show you a couple of examples of this later.

This slide is Zeng Jinyan. She is the wife of Hu Jia, who is a famous activist. He was nominated for a Nobel Peace Prize, and she won the *Time* Woman of the Year award a few years ago. She's pretty much under house arrest and gets followed everywhere by state security, so this is her way of giving us a window into her life.

continued on page three

continued from page two

This photo is one of the anti-censor word plays that became very big. In Chinese the characters for “river crab” is *he xie*. But it also sounds like the words for “harmonious.” Hu Jintao’s shtick is the harmonious society. So this is one way in which Internet users in China were making fun of it.

Jiang Zemin, the previous president, came up with something called the “three represents,” which, until today, I don’t really know what they are. And I asked regular Chinese citizens and they don’t really know what the three represents are either. But it’s called *san ge dai biao*, which sounds like “three (people) wearing watches.”

So basically, you have the river crab wearing three watches. It’s something that isn’t immediately obvious. But that’s how Chinese Internet users went under the censors’ radar.

Adapting to Internet Changes

In 2002, I began my AP tour in China. One of the ways that I talked to dissidents and activists was via your regular, old school way, where I tried to meet up with them or called them on the phone. But that changed as the years went by.

Then I went to e-mail and texting, to be a little more

Nothing is ever secure. The activists and journalists have to keep up with how the Internet keeps changing

secure. But obviously, that didn’t work. And by the time I left, I was using Skype. You just have to do the best you can. Nothing is ever secure. Or at least that’s the assumption, to keep people safe. The activists and journalists have to keep up with how the Internet keeps changing.

YouTube Video

I’d like to leave you with a very quick video on YouTube. I must warn you that there’s really strong adult language in it, so please don’t be offended. I chose to show this because it underscores just how dissatisfied many people are with the kind of censorship that’s proliferating. The video is a riff on the *cao ni ma* (grass mud horse), which is a mythical creature made up by Chinese Internet users that looks like an alpaca. But it also sounds like the word for some unmentionable act that you do to someone’s mother.

This grass mud horse lives in a land that eventually gets overrun by river crabs. So basically, the video is about Internet censorship and how the river crabs, meaning the Chinese government, is infringing on one’s basic freedoms. It’s also sung by children. It sounds like a

happy little song about grass mud horses, but the English subtitles—again, I apologize—give a very different meaning. The video went viral for quite a while before the government censors got wind of it.

[See <http://www.youtube.com/watch?v=wKx1aenJK08>]

LIEBERTHAL: There is a phrase that is familiar to anyone who has studied China that means, “The center has its policies and the localities have their countermeasures.” It sounds to me like the Internet censors have their policies and the Internet users have their countermeasures. One of the issues we’ll want to discuss, inevitably, is whether a balance is emerging between the two in this struggle over access to information.

Irene Wu is next. She is Director of Research in the International Bureau of the FCC. Her presentation actually complements very nicely what we just saw. She’ll introduce basic information on how to think about understanding the Internet in China and key resources that are available to understand developments in the system there.

WU: Thank you, very much. And it’s hard to follow a YouTube video like that. I am from your friendly neighborhood regulator. When people complain about us, they usually don’t show alpacas. They call us by name and they file a comment on our website. So it’s a different world.

I’d like to introduce at least one conceptual tool to give you a sense of how we in the communications world are beginning to view information and information flows across the world.



Dr. Irene S. Wu, Director of Research,
International Bureau, Federal
Communications Commission

Second, I will touch a little bit on the structure of Internet censorship and the authorities who are involved in China. Third, I’ll name a few of the issues that are typically at stake when we discuss censorship and filtering over the Internet. And lastly, I have a few practical tracking tools for those of you who might be interested in following this on country-by-country or regional basis.

[Irene Wu’s Power Point presentation is available at http://www.eastwestcenter.org/fileadmin/resources/washington/usapc/Wu_Tips_on_understanding_Internet_censorship_1.ppt]

It’s common for us to talk about information as power
continued on page four

but I wonder how we can think about this idea to make it a practical device to use in our everyday understanding of the Internet and politics. I have a comparison between economic power and information power. We think of a country's economic power as resting on its markets, its income, usually measured by GNP. The currency is money or capital.

And the idea of a socioeconomic class is really the nexus between economy and society. When we walk into a country and try to understand what's going on, we easily organize that society into different classes—usually high, middle, and low class. When we observe a major shift from, say, the people who belong to the low class, to the middle class, then we understand that there are implications for the political system and, in terms of international relations, perhaps a reprioritization of national interests.

Nodes of Connection

I would argue that we can extend this concept to information power. We can think of the network as the analytical unit, not just the physical infrastructure but the human beings, the people who are connected by this infrastructure. So in that information network infrastructure, there are those that create connections. And for ease of use, let's call them nodes. So we're all nodes here on the panel.

The East-West Center is a node, spreading information about foreign policy and trade policy. The government is typically a node, able to create special kinds of connections. And a company like Google or Bing is a node, as well, and a search engine, that really makes it possible for people to make connections, that would otherwise would not be possible.

Networkers

Then there are the networkers, who transmit information. So suppose *The New York Times* breaks a story. Then bloggers around the world transmit that information to their readers. Or perhaps a university breaks new ground in terms of its research. Then the media and policy makers start to work on those implications. And you can see here the flexibility of this concept. Today I'm a node. Tomorrow I'm a networker.

Off the Network

The third category, which we're not so much talking about today but I think is also important to keep in mind, is composed of people who are not connected. They're switched off. They're off the network. And just as in the international trading regime, sometimes there's an ideological reason for this. North Korea, Burma—there's a rea-

son why they're cut off from both the international trading system and international information networks. It's an ideological reason. In other cases, people are cut off because there's a lack of access. Maybe there's a poverty of resources, a poverty of time, or a poverty of attention. So this is a whole other community that I believe is deserving of attention in international development.

Applying the Tool

Let's try applying this tool. Suppose that the Chinese government is at the center of its network, as are many other national networks. Then, to take one case that's very current, there are the Google networks. There's google.com, which many of us use in the United States. There's google.cn and google.hk. All these information and search networks have some overlap.

When there's some tension, perhaps between the government and a particular Google network, like the google.cn network, and one of them goes down, then what is happening? You have a shift of people from one information network to other information networks. And you can predict that this will have the kind of impact on people's lives and on the prioritization of their interests that it would in an economic context.

To apply it from a different perspective, maybe I can ask you to participate in an exercise. I'm going to name a few applications. And if you use them, please raise your hand and we'll see how many people are connected.

So how many of you use Blogger? Yes, we have a few! All right. Google Docs? Google Maps? A Gmail account? Some of you may have that. Some of you use Google search from time to time? All right, then we get nearly the whole room.

So then, you might consider yourself part of the Google network. I would suggest to you that if there's an attack on the Google network, then how would you feel? Based on your own experience, you may decide to stay or you may decide to leave. That's what is at stake when there's friction between these kinds of networks.

Chinese Censorship Entities

O.K., enough of the theory. Let's move on to something practical. I've identified a sampling of the government entities in China that have some relevance to Internet filtering and Internet censorship. The Ministry of Industry and Information Technology licenses telecommunications companies and issues licenses for Internet service providers. The State Administration for Radio, Film, and Television is responsible for audio-visual regulation, not only for radio, film, and television but also for the Internet.

The Ministry of Culture issues licenses for Internet cafes. The State Council Information Office has some

continued on page five

continued from page four

oversight responsibility for news, especially news about China to the outside world. The General Administration for Press and Publication has oversight of news, especially news inside China. The Propaganda Bureau of the Chinese Communist Party is responsible for ideological discipline.

And just to give you a sense of the nexus between the party and the government, when I meet with my counterparts in the State Administration for Radio, Film, and Television, on one side of the business card is their official title and their office and on the other side of the card is their rank and title in the Chinese Communist Party Propaganda Bureau. So these are very closely tied entities.

The China Internet Network Information Center very usefully does regular surveys of Internet use in China. It's a good place to go for the numbers of subscribers. The Center also is responsible for issuing domain names. Everything with a .cn extension is issued by them.

Local and National Campaigns

Tiao-Kuai is just a reference. To those of you who are familiar with the structures of governance in China, there is applicable in the Internet arena the same kind of structure. This means that the Ministry of Education also will have responsibility for educational Internet networks. *Kuai* refers to the fact that across the provinces, regulators may undertake Internet filtering campaigns at the local level, not just at the national level.

So to look at this issue in terms of the variety of concerns that arise, I think what Ms. Ang talked about, in terms of individual freedoms, is really the most obvious. She also touched on the freedom of the press or, as we increasingly say, the freedom of the media.

I would just point out that what constitutes a definition of media is evolving. We've usually thought of media as newspapers and television but I think a search engine is a kind of media company. An enterprise like Apple, which is a platform for applications, is also a media company. The definition of media is very much in flux, so as Internet filtering and Internet censorship are discussed, I think it's important to keep that in mind.

The New 'Reporter'

The other piece that's also evolving is the definition of a reporter. Is it just a journalist with press credentials, possibly issued by the government? How about citizen reporters who uncover corruption or manage to take a video of a crime

When you begin to consider protections, I think the definition of a reporter also is very much in flux. Even here in the United States, we are questioning whether a

blogger is a reporter and what protections would apply.

Commercial Concerns

There are commercial concerns that come into play. For example, in the United States when we talk about network management, it's usually a concern about commercial issues. If an Internet service provider is affiliated with a television producer, are they able to give priority to that producer's television programming? Are they able to degrade the delivery of programming from a rival television source? The technical tools for this kind of network management and Internet filtering and Internet censorship are all very similar. What really distinguishes among them is the motivation.

Across the provinces, regulators may undertake Internet filtering campaigns in addition to controls that have been imposed at the national level

Regulating Cultural Content

Those of you who've worked in the audio-visual area know that even democratic governments sometimes have quite extensive content regulation. The purpose usually is to promote one's own culture and language or perhaps to ban certain kinds of harmful influences. Australia, very recently, just started filtering the Internet to protect its citizens from child pornography.

Over time, we are beginning to observe, as regulators here in the United States, that national regulators are beginning to transfer the kinds of rules that they have for television, radio, and newspapers over to the Internet. This is a gradual progression and you would expect to see this happen in many parts of the world. It's not surprising, then, that this would occur in China.

National security, is the subject of Jim's speech, so I will not address that issue.

Organizations Tracking Censorship

Finally, this slide provides a sampling of the kinds of organizations that are tracking Internet filtering and censorship around the world. The Open Net Initiative is a collaboration between the University of Toronto and Harvard University. It has country-by-country reports about Internet filtering, particularly for political reasons. Reporters Without Borders has an Internet predators map, which is very exciting. You can see they focus not

continued on page six

continued from page five

only on authoritarian regimes but all kinds of regimes that have restrictions.

Google itself has a map that lists all the requests from governments that they receive to take down content. It can be very instructive to take a look at that. The Open Society Institute has reports, as well. They focus not only on filtering and censorship but also on the value of information to good governance in a digital age. And finally, there are regular reports from the Freedom House.

LIEBERTHAL: Thank you, very much. Our final presenter, Jim Lewis, turns this equation around and considers choices that the Chinese government makes and some contradictions that it must address in making those choices. These include: (1) how one balances openness, which brings political risk, against control of information, which may undermine Beijing's high-priority goal of seeking innovation; (2) whether to take a national or a global approach to information technology; and (3) how to weigh the immediate benefits of cyber-espionage against the risk of long-term damage to U.S.-China relations and to China's own information structure from retaliation by the United States.

Jim is Director and Senior Fellow for Technology and Public Policy program at the Center for Strategic and International Studies.

LEWIS: Thank you. In some ways, it's hard to talk about the national security aspects of this because the field is relatively new and it's marked by bad data, no data, wild hypotheses, self-interest, and exaggeration. But other than that, we're off to a good start. Oh, the terminology is also imprecise.

So I want you to dismiss the terms "cyber-war" and "cyber-attack." There has never been a cyber-war and I know of only one cyber-attack.



Dr. James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies

Well, that's not true. I know of three or four cyber-attacks. The most public one was the Israeli attack on the alleged Syrian nuclear facility.

So we're not here to talk about war or attack. We're here to talk about what the Chinese government does

and why they're interested in this.

The primary goal of their efforts in the information space, as all of you know, is to see that the party retains its control and that the regime survives. So there's been an immense investment in controlling information. The multi-billion-dollar Golden Shield initiative basically

enables the Chinese government to eavesdrop on its own citizens with capabilities like those of our National Security Agency.

Economic and Military Purposes

The secondary goal of this effort is collection of information for economics and military technology. It's traditional espionage. China has had a long-running technical collection program to acquire intelligence and technology which, in turn, provides economic benefit as well as enables the traditional reasons states engage in espionage. But they also look at activities that could affect the survival of the regime.

Google and Intel

So the controversy earlier this year involving Google, was interesting because it blended both motives—a strong interest in Tibetan human rights activists as well as a desire to acquire Google's technology not only to reinforce Baidu [the Chinese search engine] but also China's own efforts to control information.

I had a conversation with some Chinese officials about the Google case and they said, "How did you know

We are beginning to see problems we've had with China's theft of U.S. intellectual property rights translated into cyberspace

it was us?" And I replied, "Name one other country that spies on Tibet. Botswana, Belgium—Stop me when I hit it."

But other companies also were hit. The one we know about publicly is Intel, the chip maker. The damage was so bad that Intel even included this episode in their 10-K report to the Securities and Exchange Commission.

Intellectual Property Theft

Some of this activity reflects traditional motives for espionage. But some of it also reflects Chinese attitudes towards intellectual property. We are beginning to see problems we've had with China's [lax enforcement and outright theft] of U.S. intellectual property rights over the last two decades translated into cyberspace. Before you had to be physically located in China to have your intellectual property stolen. Now you can live here in the United States and enjoy the same benefits without travel.

The other issue is indigenous innovation. This is an interesting problem because the Chinese have a conflicted approach towards indigenous innovation. They don't like

continued on page seven

continued from page six

using Western technology. They're convinced that America builds backdoors and traps and honey pots and Trojans into its software.

Indigenous Innovation

So they've been pushing very strongly for about two decades to develop their own IT industry. They identified this sector back in the 1980s as a crucial industry. And one of the reasons was not only the potential for economic growth, but also the military and security implications.

The Chinese don't like depending on Western technology. They're not yet at a level, however, where their own technology works. And so when you talk about things like Green Dam or WAPI [WLAN Authentication and Privacy Infrastructure] these are Chinese technologies which, if they had been implemented, would have made China more vulnerable.

There's a real tension here. "We don't like depending on the Western stuff but, if we use our own stuff, we might be worse off," is the view. So one solution is to steal the Western stuff.

Business Warnings

There are problems here that the Chinese leadership has to confront and I want to talk about them. But let me give you an example. This didn't get that much attention in the United States but, on two separate occasions, the British Security Service, MI-5, has issued warnings about doing business in China.

They've told British companies that if you do business in China, expect that your Chinese counterpart will have made some effort, using cyber techniques, to acquire your playbook, your bottom line, your negotiating position—basically, they will know everything that's in your briefing book. This is part of doing business in China.

In the Rio Tinto case involving alleged spying in China by an Australian executive and three Chinese employees, there were 200 efforts by an unknown foreign entity to break into the Rio Tinto defense team network. So this also is part of doing business in China, and I think it's an issue.

Ambiguities

Let's talk about some of the ambiguities. There is openness, which brings political risk. When the Chinese first brought the Internet into their country almost 20 years ago, this is what they were focused on. "How do we architect this new technology in a way that will limit political risk and enable us to control the flow of information?"

But at the same time, they realized that for business,

science, and innovation, they also need to be open. How do you close off the political risk and still be open for business and science? Hard to do, right?

There's this desire to co-opt and to accommodate the growing political influence of the netizens. Green Dam is a good example in this regard. I was talking to some Chinese officials and they said, "We really wanted to do Green Dam, but pressure from our netizens forced us to give it up."

However, the Chinese do not give up when it comes to extending control through technological means. There's a two-to-three-year cycle. They try a new technology. Everyone beats them off. Two years later they're back trying it again. So Green Dam went away. It should be here in about 16 months.

National vs. Global

There's this issue that I refer to in an extremely shorthand manner as national versus global. The Chinese want to have strong national industries, national innovation, and national technologies, but at the same time, they want to be a respected member of the global community with globally competitive companies.

Well, you can't do both. You cannot have national standards and yet be globally competitive. Consequently, the Chinese have been reluctant to go into the international standards-setting bodies because some of their standards don't work. If you put them out for peer review, the peers say, "What's this? Take it away!"

In this regard, it is interesting to observe that in the last year or so, China has made a huge effort to send large numbers of people to these international standards bodies. But there's still a debate in the China about whether a national approach or a more globally oriented approach to information technology and innovation makes sense.

Cyber-Espionage

Cyber-espionage has the potential to become a major problem in the bilateral relationship. Some people are deeply upset the Chinese are spying on us. Come on! That's like being an Orioles fan and complaining that the Yankees score runs. It's not that the other team is trying to score runs so much as the fact that our defenses are bad.

Until we fix our defenses, there's this temptation on the part of China to continue to use cyber-espionage. They use proxies. We've just described this immense system to control information and Internet access in China, yet we are asked to believe that there are cyber-criminals who have escaped the control of the government and are patriotic hackers. That's nonsense!

Yes, there are people who sometimes escape control. But these cyber-criminals are largely proxies for state

continued on page eight

continued from page seven

activities. You saw this in the Google case. You see it in Russia and other places too. It's a fairly common technique.

But as the Chinese continue to reap the benefits of cyber-espionage and economic espionage, they need to think about the potential damage to the bilateral relationship as well as its relations with other countries around the world. The key issue is how will China relate to the rest of the world? How will China fit into the global information infrastructure? The Chinese themselves have not sorted out these questions yet.

Potential Cooperation in Fighting Cyber-Crime

There's the issue of what happens to our own information infrastructure if we keep doing what we're doing. Again, this gets back to intellectual property protections. We've been very damaged by poor intellectual property protection in China.

But it turns out the Chinese have been hurt as well. You cannot have secure networks if that security is based on pirated software. One of the reasons is because much of the pirated software comes from the Russian mafia.

To give you a current example, Xinhua, the Chinese news service, was hacked today. If you go to their website and click on their news center, you will also install malware on your computer. This isn't a Chinese government plot. They're probably as embarrassed as we would be. The Chinese are beginning to suffer as much from cyber-crime and cyber problems as the United States. And so they're beginning to look for ways to cooperate.

Political Impact

The impact of the Internet and technology on politics is very hard to predict. The Internet has expanded participation in China. It has created a degree of transparency. There are new forces as a result. But I don't think I would call this necessarily democratic in the Western sense.

To wrap up, there is a very complex set of issues involving political forces in China, tensions in the relationship with the rest of the world, and hard strategic issues on both security and economics, innovation, and research that will take some time to work out.

LIEBERTHAL: Thank you, very much. I've begun to get involved in this area and my own sense is, when you begin to learn what has been acquired, in terms of information that should not have been acquired, from U.S. servers by what appear to Chinese entities, it's enough to make you gasp. And then, when you get into it deeply, your initial gasp looks like a mild sigh, as you really begin to try to keep your lungs working.

The question in my mind is whether the Chinese can

integrate and utilize the information that they collect relatively effectively, or whether they have the kind of problem that we long have had. That problem is knowing how to channel pertinent information to folks who can actually use it and delivering it in a way that is readily usable.

The challenges are not as much on the collection side as on the delivery side. It's everything you've done after you've brought in that new Library of Congress-worth of data in the last hour.

This is an issue I wish we knew more about.

Let me pull together a little bit what we've heard here and then open it up for your questions and comments.

Fundamentally, in China we're dealing with the world's

largest Internet community, roughly 400 million people, give or take. What hasn't been said but I think everyone understands, is that the Internet has helped make Chinese society amazingly vibrant.



Dr. Kenneth Lieberthal, Director, John L. Thornton Center, The Brookings Institution

Vitalizing Effect of Internet

If you access the Internet in China, you will find that there is a hugely diverse, excitable, fascinating world out there, very different from anyone's monochromatic view of China—or even a view of the colorful areas of Shanghai or Guangzhou. This is striking.

But the Chinese authorities do not have a very liberal approach to what they would like to see the Internet do and not do. They have a lot of tools available to try to shape what the Internet actually becomes. And society, in its various particulars, tries to find workarounds.

My guess is that most Chinese aren't so concerned with the workarounds. They're enjoying what they can access. So I think we tend to focus on those few who are really unhappy, which is a small percentage in China but still a large absolute number.

But I think most people access the Internet in China for sex, sports, and commerce, like they do in the United States. The authorities try to block sexual content, but sports and commerce are fine. And a lot of the sex seems to get through, too.

This is a highly dynamic, contradictory, roiling part of the world, that can certainly impact our world, not only through espionage and violation of intellectual property rights, but also through China's efforts to create global standards around encryption and the effect of pirated goods that flood into our markets. We're dealing with something that is very dynamic and very consequential.

continued on page nine

continued from page eight

With that brief summary, the floor is open to any questions that you would like to raise to any of our panelists.

QUESTION AND ANSWER PERIOD

JAMIE METZL, The Asia Society: My question is for Ms. Ang. You mentioned that there is a large group of bloggers in China who are being paid by the Chinese government. We also hear Chinese government officials saying, "You're lucky that we're holding back the tide of this crazy Chinese nationalism, anti-West, anti-Americanism that's coming from the blogosphere."

Is that one and the same? Do you believe that China is creating a straw man out of these crazy nationalist bloggers to make them seem like the good cop compared to that bad cop??

ANG: That's an interesting question. Actually, I said people. They're not just bloggers that are hired but commentators or people who drop in responses to what bloggers would say.

I can only speak from my experience. It's such an unwieldy tool, the Internet. But, yes, from what I've seen, I think the government sometimes works around the situation. For example, there was an anti-Japan protest a few years ago. The Chinese government allowed that tide of nationalism because in some ways it worked for them.

But then I think they realized what a huge tide this could become and how fast it could turn and that's when I think they start reining things in. So, yes, I think the Chinese government will allow things to get a little crazy if it suits their purposes. But they will very quickly shut it down as soon as they feel like they're losing control.

In terms of the government managing the debate, these people who are paid or the volunteers do kind of shape the discussions in a certain direction. They perform a type of crowd-control mechanism.

If a discussion's going a certain way that is going to be critical of the government, these commentators will step in and move it in a less dangerous direction. But again, you know, it really depends on the situation and the particular province.

UNIDENTIFIED SPEAKER: Did you observe any conflicts between provincial and central government censorship. Has there been local censorship that the central government subsequently opposes? Are they censoring each other?

ANG: What you're asking is kind of how it all works in general. Yes? For example, in 2007 the central government loosened restrictions on reporting. So technically, we could go report anywhere we wanted and interview anyone we wanted as long as they gave us permission

and they knew who we were. So that's the state law.

But the provinces, the counties, the towns, and the villages go by their own rules. And so we could say, "Look, we're allowed to do this." And they might say, "We don't care. In our town, you're not supposed to be here. Get out."

There is this dichotomy of what is supposed to be and what actually happens. China's such a huge country, so whatever is said on top isn't necessarily practiced at the bottom.

WU: I mentioned this in my presentation. I can just give you the reference. I have hard copies here. There is a paper by Henry Hu that discusses how at the provincial level the regulators are able to conduct campaigns on certain kinds of Internet content separately from other provinces.

I haven't seen it myself but that would imply that in certain provinces you would be able to see certain content and in other provinces you wouldn't. And you could predict which provinces would be more open and which ones would be more closed.

ANG: In general, the southern provinces are a lot more open. You see that in the newspapers too. They're a lot more daring. They take more chances.

EUGENE MARTIN, Asia-Pacific Strategies: Why should we be surprised? China has always controlled information. They've always insisted upon the party having control over public opinion and expressions of public opinion. We've all thought over the last few years, "Aha. The Internet's going to be the magic key that opens up China to the world." But the party has constantly had one main view and that is that they needed to use all the instruments of control over information to maintain its position and power. It's not a question. It's just a statement, I guess.

WU: What you're saying is absolutely true. And as I mentioned, in countries throughout the world, whatever policies they had towards news and information and audio-visual content for newspapers, television, radio, and films are now being transferred to the Internet. So in that sense, Chinese authorities are being completely consistent with their last 50 or 60 years of policy towards information.

The thing that you experience with the Internet that is different from newspapers and television is that there's an interactivity in this communication which also exists with other media but its not so immediate.

So, for example, with a newspaper, you do have letters to the editor, but the process for responding to these letters is filtered. The editor may see them, but the public may never will. You don't get that sense of immediacy

continued on page 10

that you do with blogs and other kinds of running commentary on the Internet. So that would be the new element.

ANG: I don't think it's surprising at all. What I find interesting is that there's this Great Firewall, but cracks that are starting to appear. This creates an element of suspense. When will it give? Or will it give? And that's the part that I find interesting to watch. You plug one hole in the wall but then other things start coming out. For me, that is what's key here.

LEWIS: There is this view that the Internet would bring democracy. And that's clearly not what's happening. And we shouldn't be surprised. You're right. But I'm not willing to dismiss it.

There are new political forces and they are empowered or created by this technology. It may not be democratic in the Western sense but, in terms of more participation or more openness, I think politics in China is different as a result. How this will play out, we can all take bets, if you want, and see who wins in ten years.

LIEBERTHAL: Let me raise another kind of layer of this that Jim alluded to in his formal remarks. The Internet was founded on the notion of one world, a global platform of free information flows. Certainly every country, in a minor way, challenges that by having some restrictions on content within their national borders.

The question is whether we now are seeing a real uncertainty about the balance that'll be struck in the future, legal and otherwise, between the notion of a global platform without national boundaries versus sovereignty extending into the digital realm. What are your thoughts?

LEWIS: That's absolutely right. We're at a transitional moment. You've all probably heard that cyberspace is a commons. I want you to imagine the mooing of cows because that about captures the intellectual content of this commons concept. It's not a commons.

Sovereignty applies to every aspect of cyberspace, because it is an artificial construct that depends on machines that are located in a country. What we are seeing now are two things. First, other countries have said, "There is this American view of a commons. Maybe that's not right. Maybe I don't have to accept the American view."

The second thing is, now that they've figured that out, they're starting to build the technologies—and Australia's a good example—that will let them extend sovereignty. We are at the cusp of seeing sovereignty extended. The issue for the United States is can we still shape that in a way that will make it more consistent with

our values rather than the values of others who may not treasure free speech as much as we do?

LIEBERTHAL: This also gets to something like Google. Just think of how much information about each of you Google has somewhere or other in its system. But

The Internet has not brought democracy to China in the Western sense, but politics are different as a result

Google is an American company. And even as an American, I'm not comfortable with the fact that Google knows more about me than I want anyone to know about me. But if I were not American, I would be even more discomfited because ultimately, Google is an American commercial operation.

I don't fully understand Google's relations to the U.S. government or the U.S. government's ability to get information from Google or any other government's ability to leverage Google for information. I use Google simply as a prominent example. This is not an aspersion on Google.

But it's a very, very tough world out there, with a lot of issues that are still not fully understood and not fully mature and resolved. So it's very dynamic.

WU: This is a moment when norms are developing. Internationally, these norms are far from settled. They touch on issues of privacy. They touch on issues of security, on the proper behavior of intermediaries, organizations that have a lot of data and facilitate the interaction between users and other kinds of commercial providers.

It's a very exciting time to be having an exchange and dialogue with other countries on this subject. Just like the development of human rights ideas and other kinds of international norms, this is something that requires a lot of talking through to get a clear understanding of where everyone stands.

JAY HENDERSON, Voice of America : Dr. Lieberthal, you mentioned Google and you mentioned sometimes you discover things about China that make you gasp and then you discover things that make you gasp even more. I just wonder about the Google compromise, the gmail accounts being limited to the human rights activists. The source on that information was Google itself. I don't understand why the Chinese authorities didn't go far beyond human rights activist into all of the reporters that covered them.

ANG: They did, actually.

continued on page 11

HENDERSON: The point is that Chinese government censorship of the Internet and e-mail goes far beyond Tibet, Falun Gong, Taiwan, and those few sensitive things. The Reporters Without Borders revealed a document that's issued every day by authorities in China, instructing them what they're supposed to censor and how they're supposed to treat stories.

They're not supposed to report about the attacks on the schoolchildren. They weren't supposed to report on the Expo, the Shanghai Expo. It goes far beyond what we assume the Chinese are out to censor. I wonder whether anybody has any thoughts on how widespread their censorship is, maybe potentially on how widespread the compromise actually was of gmail and Google.

ANG: For daily news coverage, the censorship changes. With respect to the earthquake in Sichuan, in the beginning, we had unfettered access, which was the most stunning thing I'd ever experienced in my seven years in China. But then as soon as questions arose about who was getting the aid or how many schools collapsed and how many children died, the censors came in. So they change the rules every day depending on what happens.

LEWIS: In terms of the extent of the compromise, you want to think of it as three layers. You have a collection program. The first thing you need to do is set priorities. We were talking about terabytes of information.

In 2007, something bad happened here in Washington. The CIO [Chief Information Officer] of the State Department, at that point, told me they had lost three terabytes of information. Well, 12 terabytes is the Library of Congress. So think of losing three terabytes of information, which would be potentially hundreds of thousands or millions of volumes of books.

The first thing I felt was immense pity for whoever the unfortunate guy was there in China who had to translate all these documents. You've got to find some way to filter out the useless stuff. And some of that is targeting. So reporters are good target; regular folks, probably not a good target. Businessmen and scientists, however, are good targets.

The second thing you have to do, then, is translate everything, which is a problem. We know that, particularly on the technical side, you can get good technical data and mis-translate it. It will take a while to work through that.

Finally, even when you get the technical data and translate it correctly, you have to figure out how to utilize it. So if you don't have the industrial processes to take advantage of the data, it's probably a three- or five-year lag.

Another factor concerns the nature of China's targeting. Their domestic effort focuses on political dissent, but their foreign program looks for economic and political targets. So the two targets don't really mesh.

LIEBERTHAL: It's one of the most intellectually inter-

esting issues out there, if you're in the government and you get involved in electronic collection and then how you make that information usable. Just think in terms of collecting more than you can conceive of at a speed that is almost inconceivable.

The challenge becomes designing a sequence of filters to get to information that's usable, but also understanding that what's usable keeps changing. You can't tell even the smartest computer just to look at the important stuff. You have to literally define it. And then you have to refine the definition. And then you have to pass it through additional filters, because you're going from millions of pages to 20 pages.

How do you select the key 20 pages, especially when you don't have one particular noun that's driving it? And particularly when most of that is oral communications? You must digitalize sounds in various dialects and various accents, from which there will be mistakes. Try noodling through that issue and you begin to realize how difficult it is, beyond simple collection, to get to real usefulness.

The worry always is, of course, that the Chinese will become very good at that. But I don't think you should assume that they're terrific at it, because it's very hard to be effective on this.

UNIDENTIFIED QUESTIONER: According to *The Wall Street Journal*, based on testimony from Admiral Blair [former Director of National Intelligence], 200,000 are Americans involved in espionage or intelligence. We haven't heard a word about what's going on our side.

Dr. Lewis, you mentioned the CIO of the State Department. Listen everybody, every CIO in the U.S. government is an agent of the one of the intelligence services.

Our computers are now being controlled by the intelligence services. And the reason that they give for doing that is to protect us against the Chinese and the Russians, because they're attacking our systems. I'm very worried that the intelligence agencies are taking over the nervous system of the United States government.



Left to right, Ms. Audra Ang, International Nieman Fellow, Harvard University and Correspondent, The Associated Press (China), and Dr. James Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies

continued on page 12

WU: May I respond? I think we've emphasized the Dark Side of the technology but I also want to emphasize, in the case of China and more generally, the openness that this technology can bring. There is a book by Guobin Yang on the power of the Internet and China. The author categorizes instances where, at a local level in China, bloggers have been able to achieve greater social justice when a corrupt official has treated someone badly or if there's been some kind of mismanagement of an environmental problem by a company.

That kind of use of the technology is very real and has a great impact on individuals' lives. It also is building a practice of collaboration and connecting a network that would not exist without these technologies.

To speak to the issue that you addressed about trying to deal with mountains of information, I was just over at the Library of Congress yesterday and the discussion there is precisely what you are talking about—how to deal with huge amounts of information and digitalize it and make it searchable. But the final step is to make it available to the public. The idea is that the public would be able to take advantage of this wonderful resource in the library.

These kinds of tools could be used for anything but they can be used, also, to open up government and to open up society. If we think of information as currency, level the information that's available to people. All right?

LEWIS: Yes, we don't want to forget the very positive effects that this network technology has brought to the world, to China and to the United States. It's created this global network for trade and business. It's created an unparalleled degree of openness, even in China.

We don't quite know how the politics of all this will play out, even in our own country, but whether we like it or not, it's here and it does seem to be having positive effects. The Dark Side of this is maybe a little more fun to talk about, but we need to remember that that's just a fraction of the whole set of events that we're looking at.

CHARLES MORRISON, President, East-West Center and International Co-Chair, PECC: We just had an international media conference in Hong Kong and there was a panel of Chinese journalists. It was quite interesting to hear the techniques that they used to get around the Great

Firewall, and particularly Twitter or the Twitter equivalents. As I understood it, in Chinese characters a lot more information can be conveyed in a very short space than in in English.

What I wanted to say, though, is that I'd had the experience of being in a city in central China one time, when monks were being beaten in Burma. At the guest house where I was staying, there were two international channels, CNN and Deutsche Welle, and everything was available, in terms of seeing monks being beaten.

When you surfed the Chinese channels, of which there were about 25, I could not see any images at all of this event. I asked the head of the local foreign affairs office what she thought of what was going on in Burma, and she said, "Is anything going on in Burma?"

I explained to her what was going on and she said, "Oh, that's why the mayor did not come to our conference." The people from the Ministry of Foreign Affairs did know what was going on and were explaining to me that the Chinese had changed their position a little bit.

But the thing that struck me is that, in a society that is more open, you see images which affect public attitudes. It isn't sustained, necessarily, but there was this outcry against the Burmese government and for sanctions against Burma and so forth.

You simply would not have that in a society that doesn't see the same images, even if you may know through the press and so forth that something was taking place. It seems that censorship has an impact on foreign affairs and on how much we can cooperate because the public dimension and the pressures in one society will be different from those in another society.

LIEBERTHAL: That sounded to me more like a comment than a question. So, great thanks to our three panelists for a series of fascinating comments and thanks to you in the audience for raising some very interesting questions. ♦



From left to right, Dr. Kenneth Lieberthal, Director, John L. Thornton China Center, The Brookings Institution, and Dr. Irene S. Wu, Director of Research, International Bureau, Federal Communications Commission

