***China Law & Policy* Interview with Dr. Adam Segal, Senior Fellow at the Council on Foreign Relations**
April 13, 2010

Transcript of April 13 Interview with Dr. Adam Segal

Hi, this is Elizabeth Lynch of China Law and Policy dot com and welcome to our podcast. For the past few months, Google's departure from China has been in the news with the focus on Google's refusal to continue to self-censor. But one area of the Google incident that has received scant attention is the cyber-attack that initially led Google to critique China's system of internet censorship. Joining me today to discuss this issue is Dr. Adam Segal of the Council of Foreign Relations. As the Ira A. Lipman senior fellow at the Council, Adam focuses on cyber-security and cyber-conflict. He is also a noted expert on China.

Thank you for joining us today.

[00:42] **EL**: *Can you just give our listeners a little bit of background on the hacking which lead to Google's announcement in January that it was looking to leave China? How widespread and sophisticated was the attack and what was the theft that Google referenced in its press release if you know at all?*

[00:57] **AS**: Google announced that it was going to be shutting down its business in China. And what they said drove them to that decision was a hacking incident which seems to have two main components. The first was, as you said, a kind of attack on Google's intellectual property, its corporate knowledge and corporate property. And the second was attacks on the G-mail accounts of human rights dissents. Google said it traced those attacks back to China; it didn't implicate the Chinese government. Others, like the New York Times have traced it back to Shanghai Jiaotong University and a computer training institute but the source of it still remains a bit of a mystery.

There is some debate about how sophisticated the attacks actually were. They were referred to as the Aurora attacks. Google has consistently said that they were extremely sophisticated but a number of other security analysts have said that in fact they were fairly basic, that much of the code used has been floating around for a long time. What the IPR that the Chinese got or were trying to get is unclear, Google hasn't specifically said. Some people seem to believe that it was basically that it was the data and databases that Google collects on its own users. So basically the kind of core knowledge that Google extracts from what Google users do, how they do it, when they do it, which would be one of the most important kind of assets that Google has.

[02:54] **EL**: *In tracing back, or Google saying that the attacks were traced back to China, why is that difficult to ascertain? To what degree…Can you put a percentage on how accurate you can trace back an attack?*

***China Law & Policy* Interview with Dr. Adam Segal, Senior Fellow at the Council on Foreign Relations**
April 13, 2010

[03:11] **AS**: The problem is that you can continually trace back the attacks to certain computers or to certain networks or IP addresses, but often once you get there, some more poking around leads you to another computer behind that. And the other thing is the hackers themselves can spoof the address that they are using. I think there becomes a fairly high degree of certainty about where the attack might have come within a national network. In some cases, even down to specific IP addresses. But even then you don't know who the hacker was that was involved and you don't know the hackers relationship to any state organization or anybody else for that matter.

[04:03] **EL**: *And in terms of China specifically, the cyber-hacking, how prevalent is cyber-hacking from China compared to other countries like Russia or even the United States? Is China being singled out here?*

[04:20] **AS**: I think China is being singled out in a sense. I mean given that it was a high profile attack on a company like Google, but also given the state of U.S.-China relations right now, that it fed into a worsening tenor in the bilateral relationship. But in raw numbers, for criminal activity, clearly Russia is very high up there and we saw the political uses of cyber-hacking in the case of the Georgian war and Estonia and some other high profile political cases. And there is a large amount of hacking that comes from the United States and that's actually one of the big complaints on the Chinese side – is that the Chinese are being scapegoated and they themselves are often victims of attacks and many of those attacks come from servers in the United States. When you look at the number of bad ISP – Internet Service Providers – that are hosting botnets and other kind of zombies that are attacking, there are a large number of them that are in the United States. So, China is also a victim.

[05:28] **EL**: *Just focusing on just China and the hacking there, can you explain maybe a little bit more what the hacker community is like in China. Is it an organized community? And what motivates the hackers – do they do this just for fun or are they ever "hired" for their skills? And also how do they determine targets – how was Google determined? Was that just something for fun or for profit?*

[05:56] **AS**: I think the community itself is incredibly hard to characterize. It's very diverse, it's, I think, very decentralized. The community represents kind of the similar community that there is in the United States and Russia. There are what they called script-kiddies – people, teenagers who are doing it for fun or to show off or to see what they can actually accomplish. There are criminals – people that are just hacking for financial gains. There are what are called patriotic hackers – people that hack websites out of a kind of nationalistic feeling. Then there are hackers that are probably employed by the Chinese government, probably by the military and the security agencies that are used to attack specific targets for political reasons. And then there are

hackers in the military that are thinking about how cyber would be used in an actual military conflict.

Of course, the important question is the relationship about all of these people and I don't think we really have a very good idea. Clearly, there is some blurring of boundaries of patriotic hackers and criminal hackers. The system itself seems to be in many ways a kind of mirror of the system that has made China such a power in the global manufacturing which is that there are kind of contracts and subcontracts and subcontracts of what people do. Somebody might be in charge of writing a very low-level code and that code is then packaged up and used by people above them, who may then might contract for a specific project or may sell it on the open market. Certain things are just put out there on hacker websites and you can just download them and buy them just for your own thing.

Why Google was targeted. If, as Google says that they were part of an attack that seems to have included at least 30 other technology companies, there does seem to be a push from Chinese intelligence community from, from its espionage community to try and get advanced technology from foreign companies. So we have seen for at least five years, if not longer, pretty concentrated, focused attacks on defense contractors and other U.S. technology providers. And then, once you add the attack on the dissidents as well, then that also seems to be one of the interests of the attacks. But who was, who within the Chinese government organized it or put it in a larger strategy, I think that we really have no idea.

[09:05] **EL***: I guess that raises kid of the other issue that has been floating around there with the Google incident and cyber-hacking in general, is to what degree is the Chinese government involved in some of these incidences? I know* N*orthrop Grumman issued a report last year to the US-China Economic and Security Commission analyzing the link between, hacking for military purposes, but this general hacking of corporations, could it be that the Chinese government is behind it? And also, when you make this distinction of political hackers, would that be motivated by the Chinese government or is it just a by-product of the nationalism that seems very active in China right now?*

[09:47] **AS**: I don't think we know. I think the most we can say is on the espionage side, it just matches, or it pushes in the same direction of a general concern we know that China has about technological dependence and wanting to gain as much technology from the West as possible. That strategy I think has been in place for fifteen, twenty years. That includes perfectly harmless, normal technology policy about how China is going to increase its own technological capabilities, goes from that to espionage and theft. You would expect that that would include the normal type of espionage or bribing, stealing, theft of secrets from corporations, to now including cyber-espionage and attacks and those things. So I would say that the government has

a role in the sense that it has set this general direction of the policy and these concerns about technology and China's desire for it. Clearly the intelligence agencies probably have a sense of specific technology that they are concerned about and want to know more about. So the hacking of the F-35 and the F-22 and those kind of things, those are clearly probably driven by government agencies who are looking at a potential conflict with the United States and want to know what those capabilities are. But once you get to the level of Google – is there a government official that says, well if we hack Google, then we can give that information to Baidu [the popular Chinese search engine] and we can have a competitor, I don't think we can know. That clearly is a possibility but at this point, it may just be criminal. It may be a criminal that turns around and says to Baidu – we can sell this to you.

On the dissident side, I think it is probably very similar also. I think in some cases the security agencies may have….are targeting specific individuals who are using those capabilities. In other cases criminal hackers go after people and then turn around and say to the intelligence agencies – we've got this person so either do something for us or pay us for the information.

[12:18] **EL**: *In the press it has often been the Chinese government attached to this cyber-hacking, but does the Chinese government ever see this cyber-hacking as a threat to its own rule either from domestic hackers or from hackers in the U.S.? Are the government agencies ever a victim of the cyber-hacking and cyber-espionage either domestically or from abroad?*

[12:45] **AS**: Yeah, I would think all of the time. I think, from the international perspective the Chinese basically assume that the United States is engaged in cyber-espionage all of the time. And that given our capabilities, in particular the capabilities that exist in the NSA – the National Security Agency – that they are….we are probably getting more from them then they are getting from us, in the Chinese perspective, and that we are constantly hacking them. So they point to that as well as to the discussions in the United States about creating a cyber-command in the military and discussions about controlling the commons and all these other things as kind of a representation of American hypocrisy. We are talking about militarizing cyber-space while they are being hacked. So I think yes, that's clearly and issue from outside of China.

On the domestic front I think yes, that Chinese government agencies and corporations are being hacked. There's been a number of prominent cases of Chinese hackers spreading malware to try and steal identity numbers and virtual money from these multiple player games. Very prominent hackers have been arrested and eventually imprisoned. So I think that is part of the threat.

The other threat is of course is that, dealing with these patriotic hackers is a double-edged sword for the Chinese government. There is a fear that while they are focusing externally, U.S. corporations or U.S. government websites, in the case of the Olympics on French websites and

things like that. But if their ire is turned inward then those people could hack Chinese government websites. I think the Chinese government is very concerned and you can see that in discussions about their own cyber-security but also trying to develop new types of software. The problem is that the Chinese is hyper-reliant in Microsoft, something like 90% of Chinese government offices use Windows. A lot of that is pirated which means that it is not updated regularly for security patches. So there is a lot of vulnerability.

[15:15] **EL**: *You make this distinction between patriotic hacking, criminal hacking, commercial hacking, but under Chinese law itself, is hacking in general illegal?*

[15:20] **AS**: It is. There are laws on the books against hacking, criminal hacking, privacy laws. Those were strengthened in December 2008 and then again in February of this year I think. The Chinese announced that they were going again to try to strengthen anti-hacking laws, in particular kind of punishment for hackers. Also on-line privacy issues and some tort issues about privacy and defamation. Like I said, there are prominent cases of hackers who have been arrested and fined. This guy who wrote this malware called Panda malware I think it was, and was sentenced to I think 3 years and fined $18,000. So there are domestic laws against it.

[16:23] **EL**: *And do you think the domestic laws are sufficient in dealing with this? And also how do Chinese laws compare to laws in the United States against hacking?*

[16:29] **AS**: I think they're comparable. I think the issue is with all laws in China has to do with implementation. Clearly the issue for the United States or other countries, investigating hacking requires more cooperation from the Chinese about, who's behind the attacks and actually following up on prosecution. But I think within China, I suspect the issue is not the law per se but expertise….all the things we have in the United States about how do you prosecute cyber-crimes – expertise at the local level, resources, enough people staffing these kinds of issues. From the Chinese perspective also, the U.S. hasn't been all that helpful either. I have heard a number of cases where the Chinese have turned around to the FBI and said –we think this hacking is coming from the United States. And the United States has not been all that responsive from what I've heard.

[17:41] **EL**: *I guess cyber-hacking, it's definitely a crime more without borders. So how do you see international law or treaties coming into play here to battle the threat of cyber-espionage?*

[17:55] **AS**: I don't think there's much to be done about espionage. There's no international treaties against espionage. We engage in it, they engage in it, our allies engage in it. I think that is likely to happen. I think espionage we have to figure out how we are going to defend ourselves against. The problem with espionage of course though is that it is hard to differentiate

espionage from what could become vandalism or an attack. So I think what we want to kind of agree on with the Chinese is that we know espionage is going to go on, but things like probing electricity grids, that should not be occurring or other kind of critical infrastructure. We should be working on how do we declare those off limits.

On the criminal front there is a…the Council on Europe has this convention on cyber-crime. I can't remember how many countries have signed it now, it's about I think 20 or 40, I can't remember exactly. But part of the problem is that most of the major players haven't signed it; the U.S. has signed it, Japan has signed it but Russia hasn't signed it. Which goes a long way in defining consistent standards across national borders about what a cyber-crime is, how do you punish hacking, create a deterrent. The problem with Russia, China things that we see as freedom of speech they see as a cyber-crime so that has been a problem in the case of Russia. But the Chinese seem to be at least studying the Council on Europe convention which often kind of the first sign that the Chinese are moving toward international standards. So I think that is a way to move forward. And within Asia itself, ASEAN has had a couple of discussion about creating a similar kind of convention on cyber-crime in the region.

And then the other issue is this international convention on arms control, on cyber-war. The United States has entered into discussions with the Russians about it. That I think is very difficult and I think unlikely to be very useful because in the kind of traditional terms of arms control verification, inspection, those are all impossible with cyber-weapons. So, that I think is useful just for talking for talking's sake but will not result in any kind of concrete agreements.

[20:53] **EL:** *Just to follow-up on the convention on cyber-crime, you said that one of the problems is definition of terms. Is that the only thing that would hold back a country like China or Russia from signing on to this kind of convention? Or are there other factors?*

[21:11] **AS:** I think that's a big one but I do think also that right now at least China and Russia find it politically and strategically useful to kind of have this arms-length relationship with hackers. As we talked about earlier, this ties the government's willingness to directly use or indirectly use hackers for their own political purposes makes it….right now that's a reason for them not to crackdown too hard on criminal hacking. So that is I think another reason why it has been hard to create a common ground.

[21:49] **EL**: *Do you think that there is any space for having maybe a bi-lateral agreement between U.S. and China or a tri-lateral agreement between U.S., China and Russia about issues of cyber-espionage like not probing electricity grids or things like that? Or do you think it would have to be global?*

***China Law & Policy* Interview with Dr. Adam Segal, Senior Fellow at the Council on Foreign Relations**
April 13, 2010

[22:10] **AS**: Well I think any convention would have to be global. But I think there is a benefit for having these bi-lateral discussions only if because this area is newly emerging and policymakers I don't think are particularly cognizant of all the risks and problems involved in any of these issues. So just having a discussion with the Russians and the Chinese and others about what the potential rules of the road might I think are probably pretty useful.

[22:52] **EL**: *Absent any kind of global agreement, how best should the U.S. government and U.S. corporations deal with this issue of their own? How can they better prevent it from happening? Or can they?*

[23:05] **AS**: That's what we are struggling with now. The United States finally has the cyber-czar in place, Harry Schmidt. I think one of the big things that is still occurring in the United States is kind of a debate about what the best metaphor for this is, how do you think about this cyber-issue. You have those like, the op-ed in the Washington Post several weeks ago by the former head of NSA, McConnell, about basically cyber-war and we're losing it and his response was very much a militarization of cyber-space. In fact he calls for something like the re-engineering of the internet so we can basically see where any attack is coming from.

And then you have Schmidt at a conference a couple of weeks ago saying – I don't believe in cyber-war, I don't think cyber-war is the right metaphor. And you have those people talking about resilience and more of a public health model for how you respond to these things – you have to defend, you have to respond, you have to quarantine.

So I think we have this broad outline, we have this debate to settle in the States. But the way we are moving is probably closer to the public health, well actually probably both tracks at the same time. From the defense side I think you are beginning to see more traction on private-public cooperation, about definitions of standards – what does secure actually mean and how should it be implemented, more spending on R&D for cyber-security, more training of people and that's a major issue is about getting people trained, more public awareness. These are all domestic issues.

[024:54] **EL:** *And just a final question. Since President Hu Jintao is in the United States, in Washington today, do you think in his side talks with President Obama, the issue of cyber-hacking and cyber-espionage will be coming up? How important do you think the Administration views this issues especially in light of the fact that Secretary of State Clinton has openly talked about it?*

[25:19] AS: I suspect it wasn't brought up in these meetings if only because over the last two and a half weeks it has been a clear effort on both sides to try to get the relationship back on

track. Clearly the Administration's major strategic concern right now is Iran and then with the currency being the second concern. So those are the two issues, from what I've heard, were discussed in the meeting. I suspect there were no reasons to bring up the cyber-issues because there are no solutions or discussion that is helpful to both sides at this point. So other than just poking them in the eye with it, I don't see why they would bring it up. So I suspect it was not discussed.

[26:09] **EL**: *Thank you very much. This was very interesting and I appreciate your time.*

[26:14] **AS**: Thank you.