National Security Group Lunch Transcript

May 6, 2013

China's Cyber-hacking

Paul Rosenzweig, former Deputy Assistant Secretary for Policy, former Acting Assistant Secretary for International Affairs, Department of Homeland Security; author, Cyberwarfare: How Conflicts in Cyberspace are Challenging America and Changing the World

PAUL ROSENZWEIG:

I enjoy coming and speaking about issues that are close to my heart. Let me remind you, Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World, available on Amazon, just type in my name. Unfortunately it is a little too expensive, but that's my publisher's problem.

I was asked to speak today about the recent report from Mandiant about Chinese cyber-hacking. As a preliminary note, I would say that while it's an important topic and we'll spend a good 10, 15 minutes talking about it and asking questions about it, we shouldn't lose sight of the fact that China is just one of the threat actors in this space. I wouldn't want the focus on China today to exclude from our consideration North Korea or Iran or any of a host of other actors. But that having been said and putting those other countries aside, the report two-and-a-half weeks ago from Mandiant, a – an American cyber security company – was really just the latest in a long line of revelations about Chinese espionage activity using cyber means. It was, however, the most detailed and the most comprehensive such report we've had at least in the last five, seven years.

Briefly what it did, for those who are – who haven't had a chance to read it, using very detailed forensics, captured over the course of five to seven years, Mandiant identified a specific pattern of activity that it called APT1, which stands for Advanced Persistent Threat 1. You should take from that, of course, that they have identified other APTs; APT2, 3, 4, 5, 6 and 7, which were not the subject of this report.

This report pretty decisively attributed the genesis of APT1, the funding of APT1 and the operationalization of it to a unit of the People's Liberation Army: Unit 61398, which until Mandiant put it in the public press, was – we are given to understand – a classified unit designation of the Chinese army. They traced the activities of this unit to a specific recently constructed building in Shanghai, Pudong new area Shanghai, with employees numbering roughly a thousand people, resourced quite significantly. Apparently it has a logistics operation. The Chinese telecoms have given this particular building a dedicated set of fiber optic T1 lines that provide the bandwidth for their operations etc. etc.

Mandiant went further than that and actually did some more forensics to identify the signatures, the operational signatures, of three specific actors from out of the thousand who work at or in this unit; actors who go by screen names of Dota, Super Hard and Ugly Gorilla, which, you know, those are the types of names that people in this space chan – choose. But Mandiant actually was able to link those screen names to the true names – the true names of three individuals, each of whom had been at one time or another a student in cyber security and computer engineering at the nearby Shanghai University, which is well known for turning out a number of very sophisticated cyber hackers, many of whom wind up going into the – we had thought would go into the Chinese military.

What they further disclosed is the extreme scope of this. I mean, there is no other way to put it. They identified over 140 US and Western countries that had been attacked and penetrated; some of them for as long as five years without knowing that they had been penetrated until Mandiant helped them figure it out. The volume of data that was stolen ranges upwards of six to seven terabytes of data, which you know, when you think about it, if you – six to 700, sorry, six to 700 terabytes – so when you think about it and you printed it out and you put it in trucks it would extend from the doors of the Pentagon to the ports in Baltimore. So, if that much data were being stolen from the Pentagon, say, or any other company in hard copy, we'd notice, right? And we'd actually do something about it. Yet what they concluded was that the surreptitious nature of this activity had pretty much concealed it for a great deal of time.

And then the last thing that the Mandiant report did, which is for the techies in the group, was they actually released about 3,000 of the threat signature and operational activity indicators that would allow users to identify whether or not they were being attacked or had been attacked. In this they were actually giving away their intellectual property. This is what they normally sell on a daily basis to companies all around America, which was very generous of them. I don't want to make it sound like they are too generous because, of course, they have also gotten the best publicity that they could ever get from this report and they will no doubt reap a great deal on the return.

The problem, really, is that this isn't news, right? It isn't news to those of us who work in the field. It is news in the public press, but reports of other institutions going back to the early 2000s in – ha – demonstrate that there have been Chinese originated hacking attacks on American intellectual property and national security information going on throughout that time. The Congressionally chartered US China Economic and Security Review Commission has been calling out China as a bad actor in this space since at least 2009 by name. That's four years ago. MacAfee, another cyber security company, did a very good set of attributions to Chinese hackers – albeit, to be fair, not to necessarily Chinese government sponsored and paid hackers – of a host of other activities. Some of the – two of the most famous in recent years, one was called Night Dragon, which was an action against US and American – US and

European oil and gas companies who were bidding on leases in West Africa. Not surprisingly we lost those bids to the Chinese National Oil Company that was aware of the bidding tactics.

And one of my favorites we – almost because it demonstrates how comprehensive and yet how trivial the topic matter can be – was one known as Shady Rat, which was operated by Beijing during the before and after of the Beijing Olympics and targeted the International Olympic Committee and the World Anti-Doping Agency, the evident purpose of which was to give the Chinese advance notice if any of their athletes had failed any drug tests so that they could be pulled from the Olympics and avoid embarrassment.

So almost everybody has, for at least five years, and now in the press the entire country, has come to understand that China is engaged in a large-scale massive industrialized cyber-hacking operation. Everybody's willing to say it – everybody except President Obama, right? Which is to say that even the most recently released policy of the administration that would – that builds a strategy for trying to protect our intellectual property here in the United States through trade sanctions and diplomatic activities – refuses to name the worst actor – or the best actor, depending upon your perspective – the worst actor in the world by name and refuses to explicitly call it out. If you believe the reporting of the New York Times, which is, you know, in terms of getting inside the Obama administration's head usually pretty accurate [AUDIO BREAK] call out our opponents, our pure opponents, for what they are, and, you know, I hadn't thought about this till I was listening to you talk, but there is a thematic consistency going on here.

So that's where we are right now and the question is what should we do about it, right? What if I were President of the United States would I do about it? What if I were a member of Congress would I be advocating to do about it? The administration seems to be moving towards a small-scale diplomatic initiative, rallying of the West to eventually call China out. That won't hurt, right, I mean, you know, diplomacy never hurts. I suspect that it won't actually change Chinese behavior. One analysis I saw, a rough back-of-the-envelope calculation, suggests that the degree of intellectual property theft in the economic domain, not the national security domain, is increasing China's GDP growth by 1-2% a year. So if you are making that much of a gain in your GDP growth, you're not going to stop unless the sanctions begin to hurt with some degree of equivalent pain, right? So it's not going to be just yelling at them that will get them to stop.

On the other hand, proposals for a full scale aout trade war, removing China's most favored nation status or slapping countervailing sanctions on all of their imports seem to be less well targeted than they might be and will have obvious adverse affects on the American economy that I am not really in a position to calculate, so I would be cautious.

If I were to stick inside the sphere that I know, I would say what is America's strategic advantage in this space? And the strategic advantage in this space – and not to exclude other spaces of diplomacy or economic sanctions or criminal charges if we can ever get these guys in America – but in this space we understand the distributed and dynamic nature of the environment. We can adapt to a non-hierarchical, non-linear structure much more rapidly than a rigid communist country. We are not perfect at it. To be sure, the US government is a very hierarchical structure itself. But we have a dynamic private sector that is the font of innovation. We have thousands, if not tens of thousands of individuals who are experts at this and truly spend their time.

So how could we take advantage of that strategic superiority for ourselves here and begin to impose costs on China that would actually, possibly convince them to rethink their large-scale theft? There is nothing else that you can call it. Here are two ideas. One I call – and I got this from a friend of mine Sam Liles at Purdue – the gamefication of counter intelligence. Chinese companies are benefitting from stolen intellectual property, but we don't know which ones are benefitting. We're not able to draw the connections between thefts of information from US oil and gas companies and direct proof of gain by the Chinese National Oil Company. That is a particularly easy case and we probably have done that one, but that is being replicated over and over again. We should simply start a game and send American hackers and American entrepreneurs out and offer a reward, right? We've got money; $10,000 for every company that you can decisively provide us forensics that show that they have profited from American stolen intellectual property. Then we can target sanctions on them. Their products don't come to the United States anymore. Hopefully, with a little bit of successful diplomacy, their products don't come anywhere near any liberal Western country of any sort, that sort of thing. Harness in effect the widespread distributed network of people who can and do understand the forensics of cyber security and get them to help us break into the – into the structure of the Chinese ecosphere, pull it apart and apply targeted sanctions in ways that actually punish the people who are benefitting from the fraudulent activity. That is one possibility.

The other possibility – and this one is a little more radical so since I am on tape I want to be clear that I haven't thought it through clearly, completely and it is just a proposal and we should think about it before we do it; but one of the things that differentiates the Chinese approach to cyber space, the cyber domain, from the American approach is that they see it as an information warfare battle space, right? Where we don't. We see information as a good and freedom of discussion as a positive value. And so we seek to foster internet freedom. China sees the free flow of information as a destabilizing activity. I actually had one Chinese interlocutor tell me that – in all seriousness – that they think Facebook is an American plot, as if Facebook would actually do anything that the American government told it to do. They believe that and that is why they worked so rigorously to control the flow of information through cyber space into their country. They don't want the destabilizing, disrupting effects to the status quo that would come from cross flows of information. That's why they built the great Chinese firewall.

The great Chinese firewall is not technologically impervious. With a little bit of effort, a covert program or maybe an overt program of the United States could start poking holes in such a wall, letting information flow. And eventually the holes would get big enough and the information flow would get strong enough that it might cause some discomfort to the government in a way that would cause them to rethink their behavior with respect to us. My motto for this program would be something like, Let one thousand tweets bloom.

That's just two possibilities. I've done my 15 minutes so I'll stop there. You can think of others if you want to, many of which would be also taking advantage of our strategic superiority in this space in understanding its dynamic nature. But I think the first and most important thing that we need to do is be willing to speak the threat that has no name, be willing to systematically and officially to say, this is China and they need to stop, publicly. We haven't done that yet, unfortunately. And with that I'll answer your questions.

WOMAN:

Thank you very much. Go ahead, on the right.

QUESTION:

So the suggestion you made, it kind of sounds like it was like a cyber security version of the Lares Marquis [PH] that we used in the early – beginning of our country, kind of where we said, hey, people with ships go out and kind of do your thing. I think that's probably – I think that's an interesting way to do it. You can really kind of combine that with a couple of different ways. Both of – kind of combine both of your suggestions, have one aspect be the more kind of subtle version that you proposed in the beginning – the first part and then as well include the – make it type of a more like a public relations thing. So basically make it so the Chinese public knows how to get through the cyber wall, make it easier for them to do so. I think that is something that we could – those two things could have a lot of good.

PAUL ROSENZWEIG:

I – I agree with you. I would make one distinction, which is my first gamefication of counter intelligence, I was looking at that mostly as collecting information and then letting the government or some official actor be the actor. If we issued letters of mark and reprisal, that is actually the old style way of authorizing some private sector actor to go out and shoot on their own and we could do that. That would be another step. That would be a significant ramp up, but we could contemplate – and some of the people in my domain have started to advocate – letting private sector companies shoot back and burn out in affect the IP addresses that the attacks are coming from. I kind of like that idea. In truth though, there's some dangers to that. There will be innocents who will be killed along the way. That's not so good. And even though I'm skeptical about the vigor with which our government is perusing this

issue, I'm not sure that I want to offload the ability to fire the first shots in the first international cyber war to Petco or Coca-Cola. I think probably we should let President Obama make that decision or any President, right?

WOMAN:

I'm going to ask a question and then we'll go back out there. How much time do we have because I know, I think the Washington Times' Bill Gertz was just talking about the potential end of the tilt to China because of the sequester cuts and other cuts, so we may be not actually having a presence there. We certainly have a lot of volatility in the region, for instance between China and the Philippines and Japan in particular. There is increasing rapprochement between China and Iran. Iran is potentially – especially now that we have agreed as a coalition to let them enrich up to 20% – they may be very soon to being able to destabilize the area. There is – there is certainly an argument, you know, to be made that we may have a year, but maybe not multiple years. And that there is another argument – I think a minority one – that we have less than a year.

PAUL ROSENZWEIG:

That's a good question. I mean the only real answer I can give you of course is I don't know. The only good news in this space that I can give you about China is that, unlike Iran, they've actually been reasonably circumspect; which is to say they are stealing lots of information, lots and lots of information, but they haven't broken anything yet, right? We suspect they have that capability, but they actually haven't done that. Contrast that with Iran, who has actually broken stuff. They went and destroyed 30,000 computers in Saudi Arabia. They were almost certainly behind the large-scale denial of service attack on the US banking system back in September-October-November last year. I don't know if you were like me, there were three or four days I couldn't get to my banking account, so that was disruptive and it was really more of a way of Iran raising their hand and saying, be careful, we have capability in this area. So, I tend to think in the cyber domain we have as much time as we do in the kinetic domain. That's not my area of expertise, but with China at least I think that the large scale cyber disruptive attacks will only follow along with a – some kind of kinetic problem of some sort, whether it is a confrontation in the South China Sea or with Japan over Sunduku [PH] and Daiwu [PH] – I don't know that foreign policy space at all, but I do think that what we see is that the – that they see cyber as a kind of combined operations piece of the puzzle, not as an independent force multiply.

WOMAN:

More questions? Yes, on the left.

QUESTION:

I'm not on the left. [LAUGHTER] It is not often heard in this room, but I wonder if we are being insufficiently paranoid. It strikes me. I have a background in the IT world for a big bank and we had a number of Chinese Americans and Chinese programmers. I know that our universities have a lot of Chinese people in IT. Is there any thought that these people may be approached by Chinese military intelligence to be a part of this exact effort and to also not just be doing this from mainland China, but to be doing it in our own backyard?

PAUL ROSENZWEIG:

That is a good question. I mean, it is an interesting one because you've actually flipped on its head what is a dominant concern of many people in cyber security academia now, which is that almost all of the students are foreign and they leave, taking their expertise with them and that we are not building a sufficient number of domestic American engineers and cyber Jedis. So, you're flipping that around right? I would answer this two ways. The first is that a lot of the software-type threats don't require proximity, so it doesn't – there is not as much value being here in the US as opposed to being in China. On the other hand, almost all successful attacks start with an insider failure and that failure can either be deliberate as in an insider who purposefully implaces [PH] malware that creates a hole in an intrusion detection system, or far more regularly, it's the product of stupidity. One of my – one of my favorite factoids from the book that just kinda blows your mind is that one of the federal government -- federal agencies did a test where they dropped these thumb drives in the parking lots outside of federal facilities. Now, everybody knows that these are a vehicle for potential malware intrusions, and you know, I use them because I use it on only two computers and I know what I'm doing but the rule is you should not plug these into your federal government computer –

MAN:

Particularly when you find these in the parking lot.

PAUL ROSENZWEIG:

Particularly when you find in the parking lot. The only thing on the test drives was a little beaconing program that reached out through the internet and said I've been plugged in, I've been plugged in, I've been plugged in! Anybody want to care to guess what percentage of our federally cyber sophisticated workforce plugged these in?

MAN:

65%.

PAUL ROSENZWEIG:

60%. If there was the great seal of the United States on it, it jumped up to 85. So the seal made them safer, you know, apparently. So – so, you know – we don't need – we don't need to worry about the fifth column when we're our own fifth column, if you will. So, we can be paranoid, but that would be the least vector of my concern.

WOMAN:

Sorry, this is just a comment, but I went to a grad school program where we had an officer in residence from the CIA and the number that he provided us was one out of every six Chinese students – foreign exchange students in the university system is already a spy.

PAUL ROSENZWEIG:

There you go. That's – that's more troubling than I would possibly know.

WOMAN:

Thank you so much.

WOMAN:

This was great. We really appreciate it. Very scary.