How the US indictment of Chinese military hackers will change cyberespionage

Updated by Zack Beauchamp on May 19, 2014, 4:45 p.m. ET @zackbeauchamp zack@vox.com

A Shanghai building that allegedly housed a Chinese military-led hacking group.Peter Parks/AFP/Getty Images

On Monday, the US government added 5 Chinese military officers to the FBI most wanted list, charging them with stealing valuable trade secrets from major American companies. It's very rare for the US to charge foreign government employees for something like this, and a major escalation in the clash between the US and China over cybersecurity.

There's no way the US will actually be able to prosecute these guys, but, according to cyberespionage expert **P.W. Singer**, that's not the point. "We're talking of hundreds of active campaigns," Singer said, "well over 100 billion dollars [stolen] from the US economy alone. The Chinese military organization [running this] has over 120,000 members." The indictment is supposed to tell China to spy less or else risk more severe punishment down the line.

BY ANY MEASURE, IT'S THE LARGEST THEFT IN HUMAN HISTORY THAT'S PLAYING OUT RIGHT NOW

Singer is the director of the Center for 21st Century Security and Intelligence at the Brookings Institute, where his work focuses on the impact of new technology on national security. He recently **coauthored***Cyberwar and Cybersecurity: What Everyone Needs to Know*, so I figured he'd be a good person to make sense of today's China news. He and I spoke by phone on the scale of Chinese spying, its impact on world politics, and whether the US really thinks that indicting a few members of the Chinese military will make a difference. What follows is a transcription of my conversation with Singer, edited for both length and clarity.

Zack Beauchamp: Let's start with the most basic question. Why did the United States just indict some members of the Chinese military for hacking?

P.W. Singer: The goal isn't to actually jail them the way it would be a traditional indictment. It's to send a message.

It's not like Seal Team Six is going to swoop into China and pull them out. It's more the symbolism of us saying "we've had enough, and we're going to air something that previously we've argued about in private."This points to the scale of concern over cyber-espionage.

By any measure, it's the largest theft in human history that's playing out right now. All this discussion and obsession over cyberterrorism, cyber-9/11 — something we spend more time on than this threat of "death by 1000 cuts." There have been over 31,000 articles on cyber-terrorism, even though there's not been a single incident that meets the FBI definition. This intellectual property theft is real.

YOU COULD INTERPRET THIS THROUGH A POST-SNOWDEN LENS

Second big message here: [the indictment] sets the table for future pressure to be brought to bear on China. It takes public things that we've had discussions about in private settings, which are then going to be pushed harder in private settings in the future. It's also notable that we didn't mention any of the state-linked Chinese companies that have been shown to benefit from this, we just named the individuals. That's a card the US can play later. So [the US] is setting up that kind of pressure in the bilateral relationship.

[It also] potentially sets the stage for action in venues that the Chinese government actually cares about. They're not sweating over what happens in a Pennsylvania courthouse so much as whether we took this to the World Trade Organization. The WTO is a setting where their economy has benefitted greatly and, if we [the US] were to take these kind of thing into a WTO setting, it could really ramp up the pressure on them.

Third, you could interpret this through a post-Snowden lens. The topic of Chinese cyberespionage had been at the top of the list in discussions for the last several years, and it was a key point that we had been trying to build pressure on bilaterally and even build an international coalition of other victimized economies for action on.

IT'S NOT TRADITIONAL ESPIONAGE THAT'S CAUSING SO MUCH DISRUPTION IN THE US-CHINA RELATIONSHIP

Then along came Mr. Snowden. The revelations kinda blew a hole in the US strategy, knocked us back on our heels on almost anything and everything cyber-related when it came to international diplomacy. This is the kind of thing that we weren't going to bring to the table in the midst of the Snowden affair playing out. It's now coming up on a year, and we're trying to show that there are other concerns on the cyber table besides just damage control.

That of course points to the very obvious way China is going to respond to this. It's going to respond with anger and it's going to respond with pointing the finger back and saying, "you Americans engage in just as much cyber-espionage as proven by Mr. Snowden." So we're going to see a public back-and-forth about this.

ZB: You mentioned something earlier about theft. About this being almost commercial, for-profit theft rather than stealing state secrets or cyberterrorism. Does China want to go after more US commercial interests than it does security interests?

PS: There is an incredible irony here. It's not traditional espionage that's causing so much disruption in the US-China relationship. It's economic espionage.

The irony is that normally we weigh national security things greater than economic security things, but in this case the scale of the IP theft is massive. We're almost saying "hey, we're OK — we're not happy, but we're OK — with your traditional forms of spying, but when you're going after trade secrets on such a mass scale, that's what really upsets us."

Alexandre Dulaonoy/Flickr

It sort of points to the new nature of espionage and national security in the espionage. It's being committed by Chinese state-linked and, in particular, Chinese-military linked entities. They're carrying out the theft. But the targets of it range from across the spectrum:

everything from jet fighter designs to oil company equipment designs to the designs of chairs made by small furniture makers. Or the theft of negotiating strategies: what everything from oil companies to soft drink companies were going to bid in competition with Chinese companies. Its been going after academic and scientific research; going even after personal cell phones.

They've gone after journalists, [as in] the famous New York Times affair where a Chinese military-linked unit entered into the Times. It wasn't after the secret recipe for New York Times newspaper ink, it wasn't after readers' credit card numbers, it was after who inside China was speaking to New York Times editors about corruption in China.

THERE IS NO ISSUE THAT'S RISING IN TERMS OF ITS IMPORTANCE, BUT IS LESS UNDERSTOOD, THAN CYBERSECURITY

The beneficiaries are everything from Chinese military to Chinese companies, who are weaving [stolen] designs into their own designs and bids. They're not paying for the R&D but they're getting the benefits of the R&D. To illustrate, this one program, the Joint Strike Fighter, was supposed to give the United States 10-20 years of advantage on the battlefield. We're not only seeing elements of the design in their new jet fighters, so the fruits of that may be becoming limited. As may sales abroad: [China] is planning to sell competitive fighter designs in foreign markets.

But this indictment in Pennsylvania wasn't about traditional national security concerns. It was Chinese companies who were competing with American steel companies, mining companies, oil companies [and] furniture companies. Both the targets and the beneficiaries of it are well beyond the traditional national security sphere.

ZB: So how big an issue is this going to be in US-Chinese relations going forward?

PS: Massive. *Massive*. There is no issue that's rising greater in terms of its importance, but is less understood, than cybersecurity. Particularly in the US-China relationship.

In the last several years, I was able to meet, along with my colleagues, with a wide range of US and Chinese officials from multiple different military and government agencies, as well as businesses across the spectrum. What was most interesting is that, when you talk to US and Chinese diplomats, they would say, "There's lots of issues that we don't agree on: borders, human rights, trade disputes. But we know how to do the dance. We know how to engage on them, we know how to talk about them. Cyber's not like that." They don't know how to do the dance yet.

A US OFFICIAL GOING OFF TO NEGOTIATE WITH CHINA ON CYBERSECURITY ISSUES ASKED ME WHAT AN ISP WAS

We don't even have the needed understanding on understanding basic terms. A US official going off to negotiate with China on cybersecurity issues asked me what an ISP [internet

service provider] was. It's a lot like going off to negotiate with the Soviets during the Cold War and not knowing what an ICBM [intercontinental ballistic missile] was. It's the same on the Chinese side.

Secondly, we have fundamentally different definitions of the same terms. You ask an American official what an "information attack" means, and they'll say it's "someone cracking into a computer network going after secrets." You ask a Chinese official what an information attack is, and they will start speaking about the spreading of rumors and false information that is 'disruptive to societal stability' such as posting bad news on Facebook.

The bottom line is that it's an incredibly tough, complex challenging issue in the relationship between the two states that are most crucial to world stability in the 21st century. Not to overstate it.

ZB: Is there any way to put the brakes on this kind of cyber-espionage? An agreement the sides can come to? A treaty? What exactly can be done about this going forward?

PS: It's all about incentives, cost versus benefits. This indictment is almost a signal to American business to be getting serious about their own cybersecurity. Not just the cyberterrorism fears, but particularly when they're engaging with China or Chinese companies on business. So make it tougher on the attacker, raise their costs.

Critical Cycles

In turn: there's attempts to signal to China that cost-benefit dynamics are not going to be the same. So far, it's been relatively costless to you and there've been great benefits. We're going to try to limit that. Taking it public, exacting some public diplomacy costs; taking it to forums like the WTO. That may now be the road for this.

This is also key signaling to other nations that have been targeted by China. I travel a great deal, and it's very difficult to find another advanced economy that isn't dealing with this. Like us, they've been relatively quiet because of worries about what it'll do to their relationship with China. No one wanted to be out front alone. [The indictment] signals that we can build a broader coalition of countries saying "This is enough. We're not going to have an economic relationship with you where we follow the rules and you don't."

THE ONE HOPE IS THAT WE SEE SOME CHANGES WITHIN CHINA

That's the point: to shore up the rules of the game, or norms, and bolster those norms with something beyond just talk. That's obviously very difficult when you're speaking about international affairs, but norms are key.

At the end of the day, though? All of these will maybe change the nature of the cost-benefit dynamic some, but it's not going to end espionage. The reality is that stealing secrets has been with us for thousands of years. It will continue to be with us for the new digital age.

That's not a happy thing to say. People want to hear that there's some kind of silver-bullet solution, be it buying a widget or winning a court case. But the reality of this is that espionage is with us, it's here to stay, all the more so as it's presently baked into the Chinese political and economic system.

The one hope is that we see some changes within China. Not just in terms of how they see external costs but, as China's economy advances, and they start to produce more of their own intellectual property, then they start to see value in protecting IP. China's economy has mostly benefitted from this massive theft, but they are starting to generate a lot of new interesting things. They're **doing cutting edge work** on everything from jet fighters to 3D printing to lasers to warships to rockets. That shifts where they lie on the spectrum, and may hopefully also shift how they start to think about the costs and advantages of IP theft.