US INDICTS CHINESE HACKERS FOR STEALING INFORMATION ON TRADE NEGOTIATIONS

DOJ just announced the indictment of 5 Chinese People's Liberation Army hackers (complete with Most Wanted posters) for breaking into a bunch of companies — and the United Steel Workers — in Pittsburgh.

I'll have more to say about the indictment later, but for now there are two parts of it I find to be particularly interesting.

The indictment was brought by the US Attorney for Western PA, David Hickton, not EDVA (the Defense Industry) or SDNY (Wall Street) where the US complains more loudly about hacking. The victims include Pittsburgh's most important companies — US Steel, Westinghouse, and Alcoa. After watching the presser, I would be shocked if Hickton is not planning on running for higher office in Western PA.

But there's another detail about Western PA that may be of interest. In addition to these blue chip industrial companies, Pittsburgh is also home to Carnegie Mellon's CERT, a public-private venture on fighting cyberthreats. That is, I suspect this indictment came out of Pittsburgh because it has the facilities to investigate such crimes.

But the other interesting aspect of this

indictment coming out of Pittsburgh is that – at least judging from the charged crimes – there is far less of the straight out IP theft we always complain about with China.

In fact, much of the charged activity involves stealing information about trade disputes – the same thing NSA engages in all the time. Here are the charged crimes committed against US Steel and the United Steelworkers, for example.

> In 2010, U.S. Steel was participating in trade cases with Chinese steel companies, including one particular state-owned enterprise (SOE-2). Shortly before the scheduled release of a preliminary determination in one such litigation, Sun sent spearphishing e-mails to U.S. Steel employees, some of whom were in a division associated with the litigation. Some of these e-mails resulted in the installation of malware on U.S. Steel computers. Three days later, Wang stole hostnames and descriptions of U.S. Steel computers (including those that controlled physical access to company facilities and mobile device access to company networks). Wang thereafter took steps to identify and exploit vulnerable servers on that list.
>
> [snip]
>
> In 2012, USW was involved in public disputes over Chinese trade practices in at least two industries. At or about the time USW issued public statements regarding those trade disputes and related legislative proposals, Wen stole e-mails from senior USW employees containing sensitive, non-public, and deliberative information about USW strategies, including strategies related to pending trade disputes. USW's computers continued to beacon to the conspiracy's infrastructure until at least early 2013.

This is solidly within the ambit of what NSA does in other countries. (Recall, for example, how we partnered with the Australians to obtain information to help us in a clove cigarette trade dispute.)

I in no way mean to minimize the impact of this spying on USS and USW. I also suspect they were targeted because the two organizations partner together on an increasingly successful manufacturing organization. Which would still constitute a fair spying target, but also one against which China has acute interests.

But that still doesn't make it different from what the US does when it engages in spearphishing — or worse — to steal information to help us in trade negotiations or disputes.

We've just criminalized something the NSA does all the time.

Update: Adding, one other reason they're probably bringing this indictment with industrials as victims is because their information is not as sensitive as Defense Contractor or Wall Street victims is.

Update: These guys are named in Mandiant's most recent report on China's hacking. So that's a lot of what they used for the indictment, presumably. But they indicted with companies that aren't as sensitive as some of Mandiant's other clients.

Update: Correction: only Wang Dong was on Mandiant's list, meaning 2 of their ID'ed people were not indicted.