HOW THE NSA DEALS WITH A THREAT TO ITS BACKBONE HEGEMONY

I have talked before about the importance of US' dominant role in global telecom infrastructure in our hegemonic position.

> US hegemony rests on a lot of things: the dollar exchange, our superlative military, our ideological lip service to democracy and human rights.
>
> But for the moment, it also rests on the globalized communication system in which we have a huge competitive advantage. That is, one reason we are the world's hegemon is because the rest of the world communicates through us — literally, in terms of telecommunications infrastructure, linguistically, in English, and in terms of telecommunications governance.

Which is why these stories (NYT, Spiegel's short version, to be followed by a longer one Monday) about NSA's targeting of Huawei are so interesting. Der Spiegel lays out the threat Huawei poses to US hegemony.

> "We currently have good access and so much data that we don't know what to do with it," states one internal document. As justification for targeting the company, an NSA document claims that "many of our targets communicate over Huawei produced products, we want to make sure that we know how to exploit these products." The agency also states concern that "Huawei's widespread infrastructure will provide the PRC (People's Republic of China) with SIGINT capabilities." SIGINT is agency jargon for signals intelligence. The documents do not state whether the agency found

> information indicating that to be the case.
>
> The operation was conducted with the involvement of the White House intelligence coordinator and the FBI. One document states that the threat posed by Huawei is “unique”.
>
> The agency also stated in a document that “the intelligence community structures are not suited for handling issues that combine economic, counterintelligence, military influence and telecommunications infrastructure from one entity.”
>
> **Fears of Chinese Influence on the Net**
>
> The agency notes that understanding how the firm operates will pay dividends in the future. In the past, the network infrastructure business has been dominated by Western firms, but the Chinese are working to make American and Western firms “less relevant”. That Chinese push is beginning to open up technology standards that were long determined by US companies, and China is controlling an increasing amount of the flow of information on the net. [my emphasis]

And the NSA document the NYT included makes this threat clear.

> There is also concern that Huawei’s widespread infrastructure will provide the PRC with SIGINT capabilities and enable them to perform denial of service type attacks.

Now, for what it’s worth, the NYT story feels like a limited hangout — an attempt to pre-empt what Spiegel will say on Monday, and also include a bunch of details on NSA spying on legitimate Chinese targets so the chattering

class can talk about how Snowden is a tool of Chinese and Russian spies. (Note, the NYT story relies on interviews with a "half dozen" current and former officials for much of the information on legitimate Chinese targets here, a point noted by approximately none of the people complaining.)

But the articles make it clear that 3 years after they started this targeted program, SHOTGIANT, and at least a year after they gained access to the emails of Huawei's CEO and Chair, NSA still had no evidence that Huawei is just a tool of the People's Liberation Army, as the US government had been claiming before and since. Perhaps they've found evidence in the interim, but they hadn't as recently as 2010.

Nevertheless the NSA still managed to steal Huawei's source code. Not just so it could more easily spy on people who exclusively use Huawei's networks. But also, it seems clear, in an attempt to prevent Huawei from winning even more business away from Cisco.

I suspect we'll learn far more on Monday. But for now, we know that even the White House got involved in an operation targeting a company that threatens our hegemony on telecom backbones.