WHEN ALL YOU HAVE IS A CYBERHAMMER, YOU HAVE TO EXPECT TO GO TO WAR AGAINST NAILS

There are two things about this NYT article describing Obama's new cyberwar policy that deserve note.

> A secret legal review on the use of America's growing arsenal of cyberweapons has concluded that President Obama has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad, according to officials involved in the review.
>
> [snip]
>
> The rules will be highly classified, just as those governing drone strikes have been closely held.

First, according to the WaPo, the government has conducted a search of any and all government officials who have had contact with the lead author of the story, David Sanger.

> Investigators, they said, have conducted extensive analysis of the e-mail accounts and phone records of current and former government officials in a search for links to journalists.

Frankly, I think the WaPo is naively ignoring the real possibility, given the updates to DOJ's Domestic Investigations and Operations Guide, that DOJ has accessed Sanger's email records directly.

Nevertheless, however they've gotten that information, the government now has a pretty

good idea who speaks to David Sanger. Presumably, folks who talk to Sanger — particularly those privy to secret workings of the White House — are cognizant of this fact.

From that I assume it's likely — though by no means certain — that the Administration is not that unhappy about having an article boasting about its aggressive cyberwar stance, even while noting that the details of it will be remain legally classified.

Meanwhile, I'm struck by this claim.

> Mr. Obama is known to have approved the use of cyberweapons only once, early in his presidency, when he ordered an escalating series of cyberattacks against Iran's nuclear enrichment facilities.

Sure, there's only been the one attack (or rather the serial set of attacks) on Iran.

But I'm struck — particularly in the wake of DOJ's filing making it clear they're investigating WikiLeaks as a spy, while refusing to tell us what laws it is using to conduct that investigation — that there has been a rather notable cyberattack whose author we don't know: the DDOS attacks on WikiLeaks as it first started to release the WikiLeaks cables, and then again last summer (a group called AntiLeaks claimed credit for the second one).

As Jack Goldsmith and Thomas Rid both point out, the Administration appears to be badly fumbling cyber defense (largely because the private sector doesn't want to play along and the Administration isn't prepared to make them), but they are very aggressively pursuing cyberoffense. Perhaps, as Goldsmith suggests, this leak to the journalist whose contacts are being monitored is intended to deter attacks on the US (though I'm not sure how a story in a newspaper that the Chinese have hacked is going to scare the Chinese from doing what they have been doing for years).

But if the US is so intent on bragging about its offensive capability, isn't it time we learned the scope of that offensive capability? Shouldn't we finally know whether the government took down a publisher's website?