THE SPECIAL SANGER CYBER UNICORN: IRAN WARMONGER EDITION

I noted earlier that the reporting on the US not imposing cybersanctions on China appears to have credulously served its purpose in creating a narrative that may have helped create the environment for some kind of deal with China.

NYT's David Sanger did his own version of that story which deserves special focus because it is so full of nonsense — and nonsense that targets Iran, not China.

Sanger starts his tale by quoting something President Obama said at Fort Meade over the weekend out of context. In response to a question about the direction of cybersecurity in the next 5-10 years, Obama spoke generally about both state and non-state actors.

> Q Good afternoon, Mr. President. You alluded to in your opening remarks the threat that cyber currently is. And there's been a lot of talk within the DOD and cyber community of the possibility of a separate branch of the military dedicated to cyber. I was wondering where you see cyber in the next five to ten years.
>
> THE PRESIDENT: Well, it's a great question. We initiated Cyber Command, anticipating that this is going to be a new theater for potential conflict. And what we've seen by both state *and non-state actors* is the increasing sophistication of hacking, the ability to penetrate systems that we previously thought would be secure. And it is moving fast. So, offense is moving a lot faster than defense.
>
> Part of this has to do with the way the Internet was originally designed. It was

> not designed with the expectation that there would end up being three or four or five billion people doing commercial transactions, et cetera. It was thought this was just going to be an academic network to share papers and formulas and whatnot. And so the architecture of the Internet makes it very difficult to defend consistently.
>
> We continue to be the best in the world at understanding and working within cyber. But other countries have caught up. The Russians are good. The Chinese are good. The Iranians are good. *And you've got non-state hackers who are excellent.* And unlike traditional conflicts and aggression, oftentimes we don't have a return address. If somebody hacks into a system and goes after critical infrastructure, for example, or penetrates our financial systems, we can't necessarily trace it directly to that state *or that actor*. That makes it more difficult as well. [my emphasis]

Sanger excised all reference to "excellent" non-state hackers, and instead made this a comment about hacking by state actors.

> "Offense is moving a lot faster than defense," Mr. Obama told troops on Friday at Fort Meade, Md., home of the National Security Agency and the United States Cyber Command. "The Russians are good. The Chinese are good. The Iranians are good." The problem, he said, was that despite improvements in tracking down the sources of attacks, "we can't necessarily trace it directly to that state," making it hard to strike back.

Sanger then took this comment very specifically directed at the upcoming Xi visit and China,

> And this is something that we're just at

> the infancy of. Ultimately, one of the solutions we're going to have to come up with is to craft agreements among at least state actors about what's acceptable and what's not. And so, for example, I'm going to be getting a visit from President Xi of China, a state visit here coming up in a couple of weeks. We've made very clear to the Chinese that there are certain practices that they're engaging in that we know are emanating from China and are not acceptable. And we can choose to make this an area of competition — which I guarantee you we'll win if we have to — or, alternatively, we can come to an agreement in which we say, this isn't helping anybody; let's instead try to have some basic rules of the road in terms of how we operate.

And suggested it was directed at other states more generally.

> Then he issued a warning: "There comes a point at which we consider this a core national security threat." If China and other nations cannot figure out the boundaries of what is acceptable, "we can choose to make this an area of competition, which I guarantee you we'll win if we have to."

Sanger then spends six paragraphs talking about how hard a time Obama is having "deterring" cyberattacks even while reporting that China and the US have forged some kind of deal that would establish norms that are different than deterrence but might diminish attacks. He also, rather curiously, talks (again) about "unprecedented" theft of personal information in the OPM hack that we need to deter — even though James Clapper has repeatedly said publicly that we do the same thing (and by some measures, on a much bigger scale).

After dispensing lots of nonsense about China, Sanger then pivots, with no transition, to Iran, beginning by refuting (sort of) NSA Director Mike Rogers' public report [see after 1:39:30, which I'll return to] that Iran has stopped hacking the US during the negotiation of the nuclear deal by claiming that Clapper said the same in secret but also said that Iran may turn to the cyber attacks it has voluntary given up.

> In classified sessions, American intelligence agencies have told members of Congress that while computer attacks on the United States emanating from Iran decreased during the negotiations over the nuclear accord, they believe that an Iran stymied in developing a nuclear ability over the next 10 to 15 years is likely to pour more resources into cyberweapons. Such weapons have already been used against the Navy, American banks, a Las Vegas casino and Saudi Arabia's largest oil producer, without setting off significant retaliation.

Sanger describes all those attacks ascribed to Iran and says there has been no retaliation (as if these attacks themselves shouldn't be considered rather pathetic retaliation against Stuxnet — which is unmentioned in the article — and aside from the sanctions and all that) without considering what it means that Iran ended them without retaliation.

A puzzle!

So having shown that, having not retaliated against Chinese hacking, the US had made some kind of deal on norms in cyberspace, and having not "retaliated" against Iran after beating it silly with StuxNet, Iran has stopped its cyberattacks against the US, Sanger then claims that Obama is having a hard time deterring Iran and China (somehow Russia, the country accused of the most recent hacks against us, has fallen out of this discussion, which I find curious).

> With both Iran and China, Mr. Obama is struggling with variants of the same problem: How do you contain a rising power that has discovered the benefits of an anonymous, havoc-creating weapon that can also yield vast troves of secret data? And how do you convince them that actions for which "they have paid no price," as the director of the N.S.A. and the Cyber Command, Adm. Michael S. Rogers, put it the other day, will no longer be cost-free?

Sanger then goes on to lay out the stakes of this, pointing to Iran's response to attacks in Iraq, Syria, and Yemen (though spinning that as its growing influence rather than US and Saudi idiocy) and China's efforts in the South China sea.

> With Iran and China, of course, cyberwarfare is only part of those middle-game challenges. Containing Iran's growing influence in Iraq, Syria, Yemen and throughout the region is central to the administration's post-accord challenge. And containing China's effort to reclaim islands in the South China Sea, a bet by Beijing that neither Washington nor Asian nations will stop it from developing a new base of operations and exclusive claims to air and sea territory, is the subtext of much of the tension with Mr. Xi's government.

That is, given our traditional conflicts with both these countries, Sanger has decided to write a very long article claiming we can't cyberdeter them, even while presenting evidence we've found some way to cyber discuss with them.

Sanger's erroneous reporting continues. First, he claims our response to North Korea's alleged hack of Sony had no visible response.

> So far, the administration's response has seemed inconsistent, and to many incoherent.
>
> When North Korea was identified as the country that attacked Sony, Mr. Obama — in possession of evidence gleaned from the N.S.A.'s yearslong penetration of North Korean networks — went to the White House press room, declared that the leadership in Pyongyang was responsible, and said the United States would retaliate at the time and in the manner of its choosing.
>
> The public retaliation was a series of modest financial sanctions that did little additional damage to the most sanctioned country on earth. If there was a lasting response to the attack, only North Korea knows about it.

This ignores that last week NSA Director Mike Rogers made it very clear North Korea has not cyberattacked any companies in the US since we did whatever we did to retaliate for Sony. Another piece of evidence that we got a country to stop, at least temporarily, which Sanger presents as evidence Obama is adrift.

Then there's Sanger's repetition of the bizarre claim that DOJ indicted a bunch of Chinese officials for IP theft last year.

> And when Unit 61398 of the People's Liberation Army in China was exposed as the force behind the theft of intellectual property from American companies, the Justice Department announced the indictment of five of the army's officers. Justice officials hailed that as a breakthrough. Inside the intelligence community and the White House, however, it was regarded as purely symbolic, and the strike on the Office of Personnel Management continued after the indictments were announced.

As I pointed out at the time, a good deal of what got charged in that indictment *was not IP theft*, but instead spying on communications during trade negotiations and disputes, something the US does itself. I mean, kudos to whatever DOJ official has gotten a slew of journalists covering cyber issues to brainlessly repeat that this was about IP theft, but it was at least as much about DOJ charging foreign officials for stuff US officials do too. It might better serve as a lesson in the idiocy of trying to retaliate against China for stuff the US does, which brings us back to the absurd notion we're going to retaliate for the OPM hack.

Jeebus.

Sanger ends this screed by focusing again on Iran.

> And now Iran is part of the worry. Admiral Rogers told a House panel that while cyberattacks directed at the United States abated during talks over the nuclear deal, the country was now "fully committed" to using them as part of a revamped military strategy. The Iranians, another senior intelligence official said, discussing private intelligence assessments on the condition of anonymity, "will be looking intensely at how we handle the Chinese."

This is, perhaps unsurprisingly given Sanger's misrepresentation of what Obama said, a misrepresentation of what Rogers said, which was [1:39;30]:

> In the 2012-2013 time frame we were seeing significant Iranian activity directed against U, they US financial sector, trying to take down financial websites. Flowing out of '13 as the negotiations kicked in in many ways we saw less activity directed directly against us, but I would remind people I

> have not seen the Iranians step back from their commitment to cyber as a tool and we see it being used against a variety of actors in the Gulf and the region, they continue to be fully committed to, how can they use this capability to achieve a broader set of national objectives.

Remember: those attacks against banks were DNS attacks, not anything striking at the heart of US financial integrity. And Iran has backed down from even that level of focus on the US. What they haven't done, Rogers' response suggests, is back down from attacks on the Saudis and Israelis (though one of Iran's most effective attacks in the US was against Sheldon Adelson's casino after he said the US should drop a nuke on Iran; the attack, which obtained intelligence, curiously took place in 2014, after Rogers said attacks against the US have stopped — does Rogers justifiably not consider this an unprovoked attack on a US company?). Which is perhaps unsurprising because Iran is involved in several proxy wars against them (especially the Saudis).

But the implication from Sanger's misinvocation of Rogers is that the US should be expected to retaliate against Iran for its use of cyberattacks in proxy wars or against entities — Israel! — that have conducted cyber acts of war on their soil.

I get that there are parts of Obama's cyber approach that need significant improvement, particularly with hardening the US government and its ill-considered rush to give corporations immunity. There are huge concerns Sanger could focus on if he wanted — as I mentioned, his silence about Russia is baffling. Non-state criminals did far more damage to JPMorgan Chase than Iran did, and non-state actors can continue to rival Iran elsewhere (as Obama said, some of them are "excellent"). But instead he chose to spin.

What Sanger has presented in this piece is evidence that the US has made progress with China, Iran, and North Korea (though in none of those cases does he admit the progress). Those are baby steps, undoubtedly, but especially with Iran and North Korea, top IC officials are the ones reporting this progress, not Sanger’s secret Congressional sources. And yet for some reason Sanger wants to misrepresent evidence and claim that this amounts to worse than nothing.