WHERE ARE NSA'S OVERSEERS ON THE SHADOW BROKERS RELEASE?

As Rayne has been noting, a group calling itself the Shadow Brokers released a set of NSA hacking tools. The release is interesting for what it teaches us about NSA's hacking and the speculation about who may have released so many tools at once. But I'm just as interested by Congress' reticence about it.

Within hours of the first Snowden leak, Dianne Feinstein and Mike Rogers had issued statements about the phone dragnet. As far as I've seen, Adam Schiff is the only Gang of Four member who has weighed in on this

> U.S. Rep. Adam Schiff, the ranking Democrat on the House Intelligence Committee, also spoke with Mary Louise. He said he couldn't comment on the accuracy of any reports about the leak.
>
> But he said, "If these allegations were true, I'd be very concerned about the impact on the intelligence community. I'd also obviously want to know who the responsible parties were. … If this were a Russian actor — and again, this is multiple 'ifs' here — we'd have to ask what is causing this escalation."

Say, Congressman Schiff. Aren't you the ranking member of the House Intelligence Committee and couldn't you hold some hearings to get to the bottom of this?

Meanwhile, both Feinstein (who is the only Gang of Four member not campaigning for reelection right now) and Richard Burr have been weighing in on recent events, but not the Shadow Brokers release.

The Shadow Brokers hack should be something the intelligence "oversight" committees publicly engage with — and on terms that Schiff doesn't seem to have conceived of. Here's why:

The embarrassing story that the VEP doesn't work

Whatever else the release of the tools did (and I expect we'll learn more as time goes on), it revealed that NSA has been exploiting vulnerabilities in America's top firewall companies for years — and that whoever released these tools likely knew that, and could exploit that, for the last three years.

That comes against the background of a debate over whether our Vulnerabilities Equities Process works as billed, with EFF saying we need a public discussion today, and former NSA and GCHQ hackers claim we ignorant laypeople can't adequately assess strategy, even while appearing to presume US strategy should not account for the role of tech exports.

We're now at a point where the fears raised by a few Snowden documents — that the NSA is making tech companies unwitting (the presumed story, but one that should get more scrutiny) or witting partners in NSA's spying — have born out. And NSA should be asked — and its oversight committees should be asking — what the decision-making process behind turning a key segment of our economy into the trojan horse of our spooks looks like.

Mind you, I suspect the oversight committees already know a bit about this (and the Gang of Four might even know the extent to which this involves witting partnership, at least from some companies). Which is why we should have public hearings to learn what they know.

Did California's congressional representatives Dianne Feinstein, Adam Schiff, and Devin Nunes sign off on the exploitation of a bunch of CA tech companies? If they did, did they really think through the potential (and now somewhat realized) impact it would have on those companies and, with it, our economy, and with it the potential follow-on damage to clients of those firewall companies?

The embarrassing story of how NSA's plumbers lost their toolbox

Then there's the question of how the NSA came to lose these tools in the first place. While the initial (and still-dominant) presumption about the release is that somehow Russia did this, since then, there have been a lot of stories that feel like disinformation.

First there was David Sanger's piece wondering about NSA being hacked — based entirely on speculative claims of three security experts (including Edward Snowden) — which nevertheless read like this.

> Snowden Snowden Snowden Snowden Snowden Snowden Snowden Snowden Snowden Snowden Snowden

Shortly thereafter, there were a series of stories based on anonymous former NSA people also speculating, which had the effect of denying that those tools would be available external to NSA in one place.

> The source, who asked to remain anonymous, said that it'd be much easier for an insider to obtain the data that The Shadow Brokers put online rather than someone else, even Russia, remotely stealing it. He argued that "naming convention of the file directories, as well as some of the scripts in the dump are only accessible internally," and that "there is no reason" for those files to be on a server someone could hack. He claimed that these sorts of files are on a physically separated network that doesn't touch the internet;

> an air-gap. (Motherboard was not able to independently verify this claim, and it’s worth bearing in mind that an air-gap is not an insurmountable obstacle in the world of hacking).

That is this story serves to deny what I and others, including Snowden, think is most likely: that someone at the NSA forgot to pack his hammer and screwdriver in his toolbox and his toolbox in his truck after he “fixed” someone’s kitchen sink or, more accurately, a forward deployment got compromised. Which would be embarrassing because we shouldn’t let forward deployments get compromised before we burn all the interesting toys and documents there. But also, we may find out, we’re not supposed to be that far forward deployed. And if we have been, we sure as heck ought not let those we’re forward deploying against find out.

We may learn more about specific targets that make this more clear, which would seem to be the extra bonus that would make compromising all these tools *and* alerting the NSA that you had them.

The impact of NSA exploiting American firewall companies should have been the subject of public Intelligence Committee oversight hearings when we learned of Juniper Networks vulnerabilities (with whispered comments about the great deal of damage those vulnerabilities had done to US agencies and companies). Given this release, the urgency of some public accountability — from both those at NSA and those purporting to oversee NSA — is overdue.