THE SPOOKS STRUGGLE WITH RECIPROCITY

I've written a lot about the norms (or lack thereof) that the US might set by indicting nation-state hackers for their spying. Notably, I was the first to formally note that Shadow Brokers had doxed some NSA hackers in his April release.

> On Friday, along with details about previously unknown, very powerful Microsoft vulnerabilities and details on the 2013 hacking of the SWIFT financial transfer messaging system, ShadowBrokers doxed a number of NSA hackers (I won't describe how or who it did so — that's easy enough to find yourself). Significantly, it exposed the name of several of the guys who personally hacked EastNets SWIFT service bureau, targeting (among other things) Kuwait's Fund for Arab Economic Development and the Palestinian al Quds bank. They also conducted reconnaissance on at least one Belgian-based EastNets employee. These are guys who — assuming they moved on from NSA into the private sector — would travel internationally as part of their job, even aside from any vacations they take overseas.
>
> In other words, ShadowBrokers did something the Snowden releases and even WikiLeaks' Vault 7 releases have avoided: revealing the people behind America's state-sponsored hacking.
>
> Significantly, in the context of the SWIFT hack, it did so in an attack where the victims (particularly our ally Kuwait and an apparent European) might have the means and the motive to demand justice. It did so for targets that the US has other, legal access to, via the Terrorist Finance Tracking

> Program negotiated with the EU and administered by Europol. And it did so for a target that has subsequently been hacked by people who might be ordinary criminals or might be North Korea, using access points (though not the sophisticated techniques) that NSA demonstrated the efficacy of targeting years earlier and which had already been exposed in 2013. Much of the reporting on the SWIFT hack has claimed — based on no apparent evidence and without mentioning the existing, legal TFTP framework — that these hacks were about tracking terrorism finance. But thus far, there's no reason to believe that's all that the NSA was doing, particularly with targets like the Kuwait development fund.

Yesterday, the spook site Cipher Brief considered the issue (though mostly by calling on CIA officers rather than NSA hackers).

But I was surprised by a number of things these men (seemingly, Cipher Brief couldn't find women to weigh in) missed.

First (perhaps predictably given the CIA focus), there's a bias here on anonymity tied to location, the concern that a hacker might have to be withdrawn, as in this comment from Former Acting Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs Todd Rosenblum.

> It can lead to the recall of exposed and vulnerable officers that are hard to train and embed in the first place.

And this, from John Sipher.

> They can arrest or intimidate the officer, they can kick the officer out of the country or can look to publicly shame or embarrass the officer and his/her country.

But the former NSA spooks who've been most vocal about being outed — notably Jake Williams, whom Shadow Brokers exposed even before he released documents with more NSA hackers identified in the metadata, but also Dave Aitel — are concerned about traveling. They largely hacked from the comfort of the US, so being doxed primarily will implicate their freedom of movement going forward (which is directly analogous to Russian hackers, who keep getting arrested while on vacation in US friendly countries). In addition to making vacation planning more complicated, doxing former NSA hackers may limit their consulting options going forward.

These spooks struggle with reciprocity. Consider these two passages in the post:

> Russian, Chinese and Iranian governments might seek to retaliate in-kind — which among authoritarian governments often rhymes, rather than duplicates, Western actions.
>
> [snip]
>
> Perhaps most importantly, the intention is part of a larger attempt to create a false moral equivalence between U.S. offensive cyber operations and those perpetrated by adversarial nation-states such as Russia, whose cyber operations leading up Western elections have grabbed the media spotlight.

And this comment from former Chief of Station in Russia Steven Hall:

> The Russians live and die by reciprocity. For them, that is one of the linchpins of how they deal with issues like these, and basic diplomatic and policy issues. Typically it has been that if we expel five of their guys, they are going to turn around and expel five of ours. They are always going to look for a reciprocal way to push back.

> But there are times were they do things that aren't always clear to us why they consider it reciprocal. And this might be one of those things.

It's clear they'd *like* to distinguish what Russia does from what US hackers do. But aside from noting that US doxing of foreign nation-state hackers comes in indictments rather than leaked documents, nothing in this post presents any explanation, at all, about what would distinguish our hackers. That's remarkable especially since there *is* one distinction: except where the FBI flips criminal hackers (as in the case of Sabu), our former spook hackers generally don't use their skills for their own profit while also working for the state. Though perhaps that's because defense contractors make such a killing in this country: why steal when Congress will just hand over the money?

Other than that, though, I can think of no distinction. And until our spooks and policy makers understand that, we're going to be the ones impeding any norm-setting about this, not other countries.

But I'm most struck by the rather thin conclusions about the purpose of Shadow Brokers' doxing, which the post sees as about fear.

> If the Shadow Brokers are in fact linked to the Kremlin, then the doxing of NSA hackers is designed to similarly impede current and former U.S. cyber operators from traveling and engaging in clandestine operations abroad — particularly should targeted countries, including allies, take legal action against the individuals for their past involvement in NSA operations. It is also designed to instill fear, as the information could potentially inspire violence against the individuals and their families.

I'm sure the doxing is about fear — and also making it even more difficult for the Intelligence Community to recruit skilled hackers.

But there are at least two other purposes the Shadow Brokers doxing appears to have served.

First, as I noted, the release itself revealed that the US continued to hack SWIFT even after Edward Snowden's leaks. It hacked SWIFT in spite of the fact that the US has front-door access to SWIFT data under the TFTP agreement with the US. Hypothetically, the US is only supposed to access the data for counterterrorism purposes, but I've been assured that the US is in violation of the agreement with the EU on that front. That is, NSA was hacking SWIFT even after the international community had capitulated to the US on access.

By IDing the hackers behind one of the SWIFT hacks, the NSA may have made it easier for other entities to target SWIFT themselves, which has increasingly happened.

More important, still, by doxing NSA hackers, Shadow Brokers likely influenced the direction of the investigation, leading the NSA and FBI to focus on individuals doxed, distracting from other possible modes of compromise (such as the Kaspersky aided third person hacks that appears to have happened with Nghia Hoang Pho and possible even Hal Martin).

More than seven months have passed since Shadow Brokers doxed some NSA hackers, even as he bragged that he had gone nine months by that point without being caught. We still have no public explanation (aside from the Pho plea, if that is one) for how Shadow Brokers stole the NSA's crown jewels, much less who he is. I'd suggest it might be worth considering whether Shadow Brokers' doxing — on top of whatever else it did to support Russia's bid for reciprocity — may have served as incredibly effective misdirection that fed on America's obsession about insider threats.