# THE DOXING OF EQUATION GROUP HACKERS RAISES QUESTIONS ABOUT THE LEGAL ROLE OF NATION-STATE HACKERS

*Update: I should have caveated this post much more strongly. I did not confirm the names and IDs released in the dump are NSA's hackers. It could be Shadow Brokers added names to cast blame on someone else. So throughout, take this as suspected doxing, with the possibility that it is, instead, disinformation.*

In 2014, DOJ indicted five members of China's People Liberation Army, largely for things America's own hackers do themselves. Contrary to what you've read in other reporting, the overwhelming majority of what those hackers got indicted for was the theft of information on international negotiations, something the US asks its NSA (and military industrial contractor) hackers to do all the time. The one exception to that — the theft of information on nuclear reactors from Westinghouse within the context of a technology transfer agreement — was at least a borderline case of a government stealing private information for the benefit of its private companies, but even there, DOJ did not lay out which private Chinese company received the benefit.

A month ago, DOJ indicted two Russian FSB officers and two criminal hackers (one, Alexey Belan, who was already on FBI's most wanted list) that also worked for the Russian government. Rather bizarrely, DOJ deemed the theft of Yahoo tools that could be used to collect on Yahoo customers "economic espionage," even though it's the kind of thing NSA's hackers do all the time (and notably did do against

Chinese telecom Huawei). The move threatens to undermine the rationalization the US always uses to distinguish its global dragnet from the oppressive spying of others: we don't engage in economic espionage, US officials always like to claim. Only, according to DOJ's current definition, we do.

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.

Remember, too, that in 2013, just two months after NSA continued to own the infrastructure for a major SWIFT service bureau, the President's Review Group advised that governments should not use their offensive cyber capabilities to manipulate financial systems.

> Governments should not use their offensive cyber capabilities to change the amounts held in financial accounts or otherwise manipulate the financial systems;
>
> [snip]
>
> [G]overnments should abstain from penetrating the systems of financial institutions and changing the amounts held in accounts there. The policy of avoiding tampering with account balances in financial institutions is part of a broader US policy of abstaining from manipulation of the financial system. These policies support economic growth by allowing all actors to rely on the accuracy of financial statements without the need for costly re-verification of account balances. This sort of attack could cause damaging uncertainty in financial markets, as well as create a risk of escalating counter-attacks against a nation that began such an effort. The US Government should affirm this policy as an international norm, and incorporate the policy into free trade or other international agreements.

No one has ever explained where the PRG came up with the crazy notion that governments might tamper with the world's financial system. But

since that time, our own spooks continue to raise concerns that it might happen to us, Keith Alexander — the head of NSA for the entire 5-year period we know it to have been pawning SWIFT — is making a killing off of such fears, and the G-20 recently called for establishing norms to prevent it.

A number of the few people who've noted this doxing publicly have suggested that it clearly supports the notion that a nation-state — most likely Russia — is behind the Shadow Brokers leak. As such, the release of previously unannounced documents to carry out this doxing would be seen as retaliation for the US' naming of Russia's hackers, both in December's election hacking related sanctions and more recently in the Yahoo indictment, to say nothing of America's renewed effort to arrest Russian hackers worldwide while they vacation outside of Russia.

While that's certainly a compelling argument, there may be another motive that could explain it.

In a little noticed statement released between its last two file dumps, Shadow Brokers did a post explaining (and not for the first time) that what gets called its "broken" English is instead operational security (along with more claims about what it's trying to do). As part of that statement, Shadow Brokers claims it writes (though the tense here may be suspect) documents for the federal government and remains in this country.

> The ShadowBrokers is writing TRADOC, Position Pieces, White Papers, Wiki pages, etc for USG. If theshadowbrokers be using own voices, theshadowbrokers be writing peoples from prison or dead. TheShadowBrokers is practicing obfuscation as part of operational security (OPSEC). Is being a spy thing. Is being the difference between a contractor tech support guy posing as a infosec expert but living in exile in

> Russia (yes @snowden) and subject matter experts in Cyber Intelligence like theshadowbrokers. TheShadowBrokers has being operating in country for many months now and USG is still not having fucking clue.

On the same day and, I believe though am still trying to confirm the timing, before that post, Shadow Brokers had reacted to a Forbes piece asking whether it was about to be unmasked (quoting Snowden), bragging that "9 months still living in homeland USA USA USA our country theshadowbrokers not run, theshadowbrokers stay and fight." Shadow Brokers then started attacking Jake Williams for having a big mouth for writing this post, claiming to expose him as a former Equation Group member, specifically invoking OddJob (the other file released on Friday that doxed NSA hackers, though not Williams), and raising the "gravity" of talking to Q Group, NSA's counterintelligence group.

> trying so hard so #**shadowbrokers** helping out…you having big mouth for former #**equationgroup** member what was name of.
>
> leak OddJob? Windows BITS persistence? CCI? Maybe not understand gravity of situation USG investigating members talked to Q group yet
>
> theshadowbrokers ISNOT in habit of outing #**equationgroup** members but had make exception for big mouth, keep talking shit @**msuiche** your next

Which is to say that, four days before Shadow Brokers started doxing NSA hackers, Shadow Brokers made threats against those who've commented on the released Shadow Brokers files specifically within the context of counterintelligence investigations, even while bragging about having gone unexposed thus far even while remaining in the United States.

Whatever else this doxing may do, it will also

make the investigation into how internal NSA files have come to be plastered all over the Internet more difficult, because Shadow Brokers is now threatening to expose members of TAO.

Which is not to say such a motivation, if true, is mutually exclusive of Russia retaliating for having its own hackers exposed.

All of which brings me back to the question of norms. Even as the US has been discussing other norms about hacking in recent years, I've seen next to no discussion about how state hackers — and remember, this post discusses NSA hackers, including uniformed members of the Armed Services, government contractors, spies, and criminal hackers working for a state (a practice we do too, though in a different form than what Russia does) — fit into international law and norms about immunities granted to individuals acting on behalf of the state. The US seems to have been proceeding half-blindly, giving belated consideration to how the precedents it sets with its offensive hacking might affect the state, without considering how it is exposing the individuals it relies on to conduct that hacking.

If nothing else, Shadow Brokers' doxing of NSA's own hackers needs to change that. Because these folks have just been directly exposed to the kind of international pursuit that the US aggressively conducts against Russians and others.

Because of international legal protections, our uniformed service members can kill for the US without it exposing them to legal ramifications for the rest of their lives. The folks running our spying and justice operations, however, apparently haven't thought about what it means that they're setting norms that deprive our state-sponsored hackers of the same protection.

Update: I forgot to mention the most absurd example of us indicting foreign hackers: when, last year, DOJ indicted 7 Iranians for DDOS attacks. In addition to the Jack Goldsmith post

linked in that post, which talks about the absurdity of it,  Dave Aitel and Jake Williams talked about how it might expose people like them to international retaliation.