

THE OTHER FACTOR IN THE DNC HACK: WIKILEAKS' PERSONAL WAR WITH HILLARY CLINTON

Since yesterday, both Jack Goldsmith and Peter Singer have had offered some interesting perspective on the alleged Russian hack of the DNC.

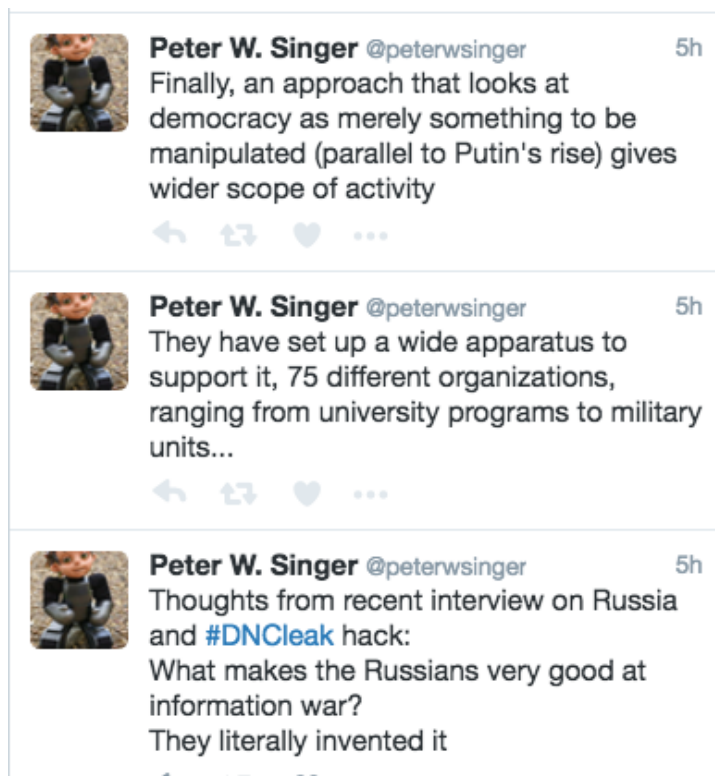
Singer had a bit of a Twitter rant.



Peter W. Singer @peterwsinger 5h
We may have to make clear we can data dump back, in ways that pressure them more...
see P. 8 of my testimony here
oversight.house.gov/wp-content/upl...

Peter W. Singer @peterwsinger 5h
3) rethink Govt approach, which is going to need to cut across from IC to FBI to State to FEC
4) rethink deterrence...

Peter W. Singer @peterwsinger 5h
What can/should we do:
1) build up resilience; don't make hacks so easy
2) greater awareness; people need to understand manipulation efforts



His linked (recent) Oversight testimony which discussed how much more complex cyber deterrence is than Cold War nuclear deterrence is.

For his part, Goldsmith first considered what was old and new in the hack, finding the only real new thing was releasing the emails.

While there is nothing new in one nation using its intelligence services to try to influence an election in another, doing so by hacking into a political party's computers and releasing their emails does seem somewhat new.

He then dismissed the notion – floated elsewhere – that this amounts to cyberwar while implying that the US has to get far better at defending our own networks and systems.

How seriously do you think the government takes issues of cyberwarfare? Do you feel confident about our defensive capabilities and competence?

"Cyberwar" is a misleading term—the Russian hack, if it is that, is not an act of war, at least not by traditional

standards. It is closer to an intelligence operation with the twist of a damaging publication of the stolen information. That said, the U.S. government takes all major cyberoperations against it and its major public and private institutions very seriously. My confidence about our defensive capabilities and competence depends on what institutions you are talking about. Today, some components of the government (e.g. the Defense Department) do better than others (e.g. the Office of Personnel Management, which recently suffered an very damaging hack). And private sector defenses, even of important critical infrastructure networks, are a very mixed bag. The scale of the challenge is enormous, and offense has many advantages over defense. I don't know anyone who is sanguine about our defensive capabilities overall.

Then he went on a Twitter rant directed at the hand-wringing about how unusual this is.

1/ In assessing the DNC hack, remember that USG is no innocent when it comes to infiltrating foreign computer networks.

2/ The cyber-attack on Iranian nuclear centrifuges was one of the most consequential in history.

3/ USG openly & aggressively supports technologies that weaken foreign gov't control over networks.

[snip]

6/ It's also well known that US has in past used covert ops to influence foreign elections.

7/ Current U.S. cyber-espionage almost certainly extends to political organizations in adversary states.

[snip]

11/ The point is that USG plays rough in cyberspace, and should expect others to do so as well.

12/ And yet USG seems perpetually unprepared. DNC hack is tiny tip of iceberg of possible electoral disruptions via cyber.

In short, both think this is something other than cyberwar, but view the importance of it differently (even while both provide suggestions for a policy framework to respond), particularly the uniqueness of the perceived sabotage of the election. But their discussion (along with virtually everyone else's) has pitched this as a two-front question, us against Russia, though Singer's testimony has a lot of discussion about how much more complexity there is to this issue, including the non-state actors who might be involved.

After having dismissed the unthinking equation of 2 intelligence hacks = Guccifer = Russia = WikiLeaks = Russia story, I want to return to it to complicate matters somewhat, to talk about Wikileaks role *whether or not it cooperated with Russia on this*. First, what follows is in no way meant to be a defense of Wikileaks' action here, which included the inclusion of credit card and social security information in the dump. ~~Particularly against the background of what it recently did with Turkish documents: in the guise of releasing a bunch of Erdogan documents, it also dumped voting information on most women in Turkey, including whether or not they were members of Erdogan's AKP.~~

~~WikiLeaks also posted links on social media to its millions of followers via multiple channels to a set of leaked massive databases containing sensitive and private information of millions of ordinary people, including a special database of almost all adult women in~~

Turkey.

Yes — this “leak” actually contains spreadsheets of private, sensitive information of what appears to be every female voter in 79 out of 81 provinces in Turkey, including their home addresses and other private information, sometimes including their cellphone numbers. If these women are members of Erdogan’s ruling Justice and Development Party (known as the AKP), the dumped files also contain their Turkish citizenship ID, which increases the risk to them as the ID is used in practicing a range of basic rights and accessing services. The Istanbul file alone contains more than a million women’s private information, and there are 79 files, with most including information of many hundreds of thousands of women.

[snip]

Another file appears to contain sensitive information, including Turkish citizenship IDs of what appears to be millions of AKP members, listed as active or deceased. Yet another file contains the full names, citizenship IDs and cellphone numbers of hundreds of thousands of AKP election monitors — the most active members of the party.

As Zeynep Tufekci points out, in the wake of the failed coup and Erdogan’s retaliation, this has the possibility of endangering a great number of people.

She blames the dump on Wikileaks’ failure to work with locals, who could have explained that the emails themselves were virtually worthless. Perhaps. Perhaps Wikileaks served as someone else’s useful idiots — or even, if you believe there’s something more deliberate behind the coup and counter-coup, perhaps Wikileaks played a more active role.

~~So Wikileaks has done two things that were egregious and damaging. I do not defend that. I condemn it (and the sloppy journalism that enabled it).~~

Update: see this post on where the Turkey files came from, which came from Phineas Fisher; it wasn't Wikileaks.

But I want to consider how different its role is with the target of this leak – Hillary Clinton (and Democrats more generally) – and Turkey.

Most of the discussion about the where and whyfor of the leak assumes it is all about Russia's interest (assuming, of course, that this was a Russian state hack). But consider why Wikileaks might want to leak in this way and at this time.

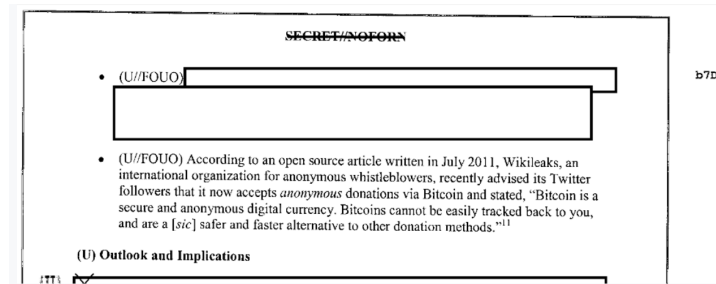
Hillary was, of course, Secretary of State when Wikileaks leaked the State department cables and pushed aggressively for Chelsea Manning's prosecution (as Charlie Savage wrote in a piece published just before I finished this, this is a point Assange made when he discussed the emails 6 weeks ago). She has, since then, been found to treat information claimed to be far more sensitive in careless fashion (as has the State Department generally).

Very importantly, State worked closely with DOJ as it investigated Wikileaks. There is very good reason to believe that as part of that investigation, DOJ mapped out Wikileaks' supporters and, possibly, financial contributors – that is, precisely the kind of people, to the DNC, that Wikileaks just doxxed. That's arguably a violation of Section 215, which includes First Amendment protections.

We also know that GCHQ was (at least as a SIGDEV research project, but those often serve to conduct surveillance that wouldn't really fly within other legal guidelines) collecting log files of people who visit Wikileaks.

We know that under pressure from the US government, traditional funding sources stopped

taking donations for Wikileaks. I've seen hints of some legally dubious action that may be worse, as well. In addition, in 2012, the FBI considered Bitcoin donations to Wikileaks among the many nefarious things one could do with Bitcoin.



Love or hate Wikileaks, but it – and its political and financial supporters – were tracked. Its sources of funding were cut off. And then the government realized that Wikileaks (at that point, at least) was engaging in what a lot of media outlets also do and conceded it couldn't charge Assange for those activities.

Now I'm not trying to say two wrongs make a right – that because FBI collected data implicating innocent supporters of Wikileaks, it is okay for Julian Assange to dox all the DNC's supporters.

Rather, I'm trying to raise this in the context of the issues that Singer and Goldsmith lay out. Whether Wikileaks cooperated with Russia (if Russia did the hack) or not, it is a key player in this leak. Even if Russia did this to help Trump, Assange executed the leaks to maximal damage to Hillary (and I suspect Wikileaks will continue to do more damage with further leaks). What does this say about issues of retaliation against non-state actors working with the sphere of state actors, as people consider information war in the era of cyber?

I don't know the answer to that, but as we raise the question, those issues need to be addressed as readily as the state actor question. The way this rolls out may be as much a question of a non-state actor retaliating against a political

figure as it is a state actor trying to elect
its preferred candidate.