JOSH SCHULTE DESCRIBED THE DAMAGE GIVING RUSSIA ADVANCE ACCESS TO THE VAULT 8 FILES WOULD HAVE CAUSED

As part of a fight over whether the government obtained Josh Schulte's explanation of his FBI interview via Schulte's prison notebooks or via subpoena from a Schulte associate (probably a family member), the government released a redacted version of that explanation, ostensibly a chapter in his "Presumed Innocent" blog. It's fascinating for a slew of reasons (including that he lays out that it would be a crime to expose the identities of his colleagues, and then does just that).

For now, though, I want to look at what Schulte claims he told the FBI about the damage sharing the CIA source code files with Russia would do (none of this appears in the 302 of the interview).

> I told them the confluence server was the one that seemed to be compromised, and while horrible and damaging at least it wasn't Stash; At least not at this point—Hopefully they could stop any additional leaks from the network at this point. From the news articles I've read, wikileaks claims to have source code, but we don't know what code or from where. However, at this point, I knew the SOP was a complete stand down on all [redacted] operations. We had no idea what had been leaked, when, for how long, or even who else had seen the materials leaked. Have they been steadily accessing our network every day? Have all our ops been blown since

> we wrote the first line of code? Perhaps only confluence had been leaked, but the individual(s) responsible are/were planning to exfil the other parts of DEVLAN too? So much still unknown, and with potential (yet unconfirmed) link between wikileaks and Russia—Did the Russians have all the tools? How long? It seems very unlikely that an intelligence service would ever leak a nation's "cyber weapons" as the media calls them. These tools are MUCH more valuable undiscovered by the media or the nation that lost them. Now, you can secretly trace and discover every operation that nation is conducting. I told them all this was certainly very disturbing and I felt bad for my friends and colleagues at the agency who likely weren't doing anything and most likely had to completely re-write everything.

I'm frankly shocked that DOJ didn't use this file in his first trial, as it accurately describes what multiple witnesses testified happened after WikiLeaks first published the leak: everything ground to a halt while CIA tried to mitigate damage. And as Schulte predicted, the Agency *did* have to rewrite everything. This is powerful evidence that, if Schulte is found guilty, he knew well what kind of damage he would cause.

Particularly given that I was told Schulte himself reached out to Russia at some point (I'm not convinced this is accurate; it may reflect a misunderstanding of discovery), I find what he said about another nation-state — and he named Russia — obtaining the documents to be particularly interesting.

To be fair to Schulte, when he allegedly leaked the documents (in April-May 2016), there was far less understanding of WikiLeaks' ties to Russia. So these comments may reflect what he understood in March 2017, after WikiLeaks helped Russia tamper in the election.

But what Schulte describes is precisely what the CIA would have been panicking about in summer 2017, as they ratcheted up spying on WikiLeaks associates. What he described with respect to *WikiLeaks' publication* is precisely what happened. With just a few exceptions (published at key moments), WikiLeaks published none of the CIA's source code. Given what we now know of WikiLeaks' ties to Russia, there's a real possibility Russia obtained the files even before the US understood the full extent of Russia's intervention in the 2016 election. As Schulte accurately describes (and I laid out here), Russia could have spent the months in the interim reverse engineering all the US operations targeting Russia and its clients.

This is something that overblown Yahoo article alluded to, but then never really considered. At precisely the moment US intelligence was beginning to understand that Assange was a Russian asset, they were never able to rule out that this is precisely what Russia did with the files.