ACCUSED VAULT 7 LEAKER JOSHUA SCHULTE PLANNED TO HAVE WIKILEAKS PUBLISH DISINFORMATION TO HELP HIS DEFENSE

When WikiLeaks announced its publication of the CIA's hacking tools in March 2017, the first tool it highlighted was an effort called Umbrage, which it claimed the CIA used to "misdirect attribution."

> ## *UMBRAGE*
>
> The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity.
>
> This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.
>
> The CIA's Remote Devices Branch's UMBRAGE group collects and maintains a substantial library of attack techniques 'stolen' from malware produced in other states including the Russian Federation.
>
> With UMBRAGE and related projects the

> CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the “fingerprints” of the groups that the attack techniques were stolen from.
>
> UMBRAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Experts noted at the time that Umbrage served mostly to save time by reusing existing code. Nevertheless, the representation that the CIA would sometimes use other nation’s tools was immediately integrated into conspiracy theories denying that Russia carried out the 2016 hacks on Democrats. Because the CIA sometimes obscured its own hacks, denialists have said since, the CIA must have been behind the 2016 hacks, part of a Deep State operation to frame Russia and in so doing, undermine Trump.

Documents released this week reveal that Joshua Schulte, who is accused of leaking those documents to WikiLeaks, believed he could get WikiLeaks to publish disinformation to help his case.

Several documents submitted this week provide much more clarity on Schulte’s case. On Monday, the government responded to a Schulte effort to have his communications restrictions (SAMs) removed; their brief not only admitted — for what I believe to be the first time in writing — that the CIA is the victim agency, but described an Information War Schulte attempted to conduct from jail using contraband phones and a slew of social media accounts.

Yesterday, in addition to requesting that Schulte’s child porn charges be severed from his Espionage ones, his defense team moved to suppress the warrants used to investigate his communication activities in jail based on a claim the FBI violated Schulte’s attorney-client

privilege. During the initial search, agents reviewed notebooks marked attorney-client with sufficient attention to find non-privileged materials covered by the search warrant, and only then got a privilege team to go through the notebooks in more detail. The privilege team confirmed that 65% of the contents of the notebooks was privileged. In support of the suppression motion, Schulte's lawyers released most of the warrants used to conduct those searches, including the downstream one used to access three ProtonMail accounts discovered by the government and another downstream one used to access his ten social media accounts (see below for a list of all of Schulte's accounts). Effectively, they're arguing that the FBI would have never found this unbelievably incriminating communications activity, which will make it fairly easy for the government to prove that Schulte is the Vault 7 leaker without relying on classified information, without accessing those notebooks marked privileged.

But along the way, the documents released this week show that the guy accused of leaking that Umbrage file that denialists have relied on to claim the 2016 hack was a false flag operation framing Russia himself planned false flag activities to proclaim his innocence.

The government's SAMs response describes in cursory fashion and the affidavits for the warrants as a whole describe in more detail how Schulte planned to adopt two fake identities — a CIA officer and an FBI Agent — to proclaim his innocence. The idea behind the latter was to corroborate two claims Schulte posted on his JoshSchulte WordPress sites on October 1, 2018 — that the FBI had planted the child porn discovered on his computer.

> i. "I now believe the government planted the CP after their search warrants turned up empty-not only to save their jobs and investigation, but also to target and decimate my reputation considering my involvement in

> significant information operations and covert action."
>
> As noted above, in the Fake FBI Document in the Schulte Cell Documents, a purported FBI "whistleblower" claimed that the FBI had placed child pornography on Schulte's computer after its initial searches of the device were unsuccessful in recovering evidence. See supra~ 14(a)(iii).
>
> ii. "So who's responsible for Vault 7? The CIA's own version of the FBI's Peter Strzok and Lisa Page,"
>
> As noted above, in the September Tweet in the Schulte Cell Documents, a purported former CIA colleague of Schulte (but who was in fact simply Schulte himself) claimed that two other CIA former colleagues, one of whom Schulte described as the "Peter Strzok of the CIA," had conspired to blame Schulte for Vault 7, WikiLeaks' disclosure of the CIA material.

As noted above, two of the documents found in Schulte's cell mixed in with the attorney-client material show how Schulte planned to create false identities to spread the same stories. One was an article he planned to send to WikiLeaks, claiming to be from an FBI whistleblower describing how Schulte was framed.

> iii. A document that appears to be an article for release by WikiLeaks.org ("WikiLeaks"), in which a purported FBI "whistleblower" claimed to have provided the discovery in this case to WikiLeaks and that the FBI had planted evidence of child pornography on Schulte's computer to frame him (the "Fake FBI Document").

The documents also include his plans to release a fake CIA tweet claiming he was framed for the Vault 7 leak.

> iv. Drafts of a tweet (the "Fake CIA Tweet") that appear to have been drafted around August 30, 2018,3 in which Schulte pretending to be a former CIA colleague claimed that two other former CIA colleagues, both of whom Schulte referred to by full name and one of whom he described as the "Peter Strzok of the CIA," had "set up" Schulte and used him as a "scapegoat" for "Vault 7," which is the name of WikiLeaks serial disclosures of CIA material that began on or about March 7, 2017 and which forms the basis of some of the current charges against Schulte. On the following page of the Schulte Cell Documents appears the text "Just to authenticate me fast" followed by other apparent draft tweets that discussed the CIA's alleged activities and methods, some of which appear to be classified (the "Fake Authentication Tweets").4 . . I believe that Schulte planned to potentially publish the Fake Authentication Tweet before the Fake CIA Tweet in an effort to purportedly verify the author's employment with the CIA and knowledge of the information in the Fake CIA Tweet.

Finally, the FBI also found Schulte's to do list of how he planned to share both the fake FBI document and his discovery with WikiLeaks.

> What appears to be a "to-do" list dated September 12, 2018, in which Schulte wrote that on September 17 and 18, he would "DL Disc. UL WL," and.that on September 19, 20, and 21, he would "schedule tweets[.]" I believe that here, "DL Disc. UL WL" means that Schulte planned to download his discovery ("DL Disc.") from the Schulte Laptop and upload that discovery to WikiLeaks ("UL WL"). As noted above, in another place in the Schulte Cell Documents, Schulte drafted the Fake FBI

> Document, a purported statement by a supposed FBI "whistleblower" who provided Schulte's discovery to WikiLeaks and claimed that the FBI had planted evidence of child pornography on Schulte's computer.

From a legal standpoint, Schulte's lawyers have disclosed all these warrant materials in an urgent effort to suppress everything the government found after first accessing his notebooks from jail. The FBI investigation proceeded from those notebooks to the WordPress site showing him claiming something identical to disinformation he was packaging up to share with WikiLeaks. They also got from those notebooks to ProtonMail accounts where Schulte offered to share what may or may not be classified information with a journalist. The reason why the defense is pushing to suppress this — one of the only challenges they're making in his prosecution thus far — is because the stuff Schulte did in prison is utterly damning and seems to confirm both his familiarity with WikiLeaks and his belief that he needed to create disinformation to claim to be innocent.

We'll see whether this Fourth and Sixth Amendment challenge works.

But along the way, the defense has released information — the provenance of which they're not disputing in the least — that shows that Schulte planned to use WikiLeaks to conduct a disinformation campaign. But it wouldn't be the first time Schulte had gotten WikiLeaks to carry out his messaging. A year ago today — in the wake of Schulte being charged with the Vault 7 leak — WikiLeaks linked to the diaries that Schulte was writing and posting from his jail cell, possibly showing that Schulte continued to communicate with WikiLeaks — either via a family member or directly — even after he had been put in jail. Those diaries are among the things seized in the search.

In a follow-up, I think I can show that Schulte did succeed in using WikiLeaks as part a disinformation campaign.

Social media accounts Joshua Schulte accessed from jail

ProtonMail: annon1204, presumedguilty, freejasonbourne

Twitter: @freejasonbourne (created September 1, 2018 and used through October 2, 2018)

Buffer (used to schedule social media posts): (created September 3, 2018, used through September 7, 2018)

WordPress: joshschulte.wordpress.com, presumptionofslavery.wordpress.com, presumptionofinnocence.net (all created August 14, 2018)

Gmail: joshschultel@gmail.com, john12galt21@gmail.com (created April 15, 2018), freejasonbourne@gmail.com,

Outlook: Johnsmith742965@outlook.com

Facebook: ‘who is JOHN GALT? (created April 17, 2018)

Update: The government also believed at the time that an account in the name Conj Khyas was used by Schulte to receive classified information at his annon1204 account. It was not listed in these warrants, but would amount to a 14th account.