

GUCCIFER 2.0: WHAT ABOUT THOSE DCCC AND “CLINTON FOUNDATION” DOCUMENTS

In this post, I addressed one recent and one not-recent research finding pertaining to Guccifer 2.0 (I had already raised both of them, but I addressed them at more length). I pointed out the conclusions of the research itself (that Guccifer 2.0 put Russian metadata in the first documents he released intentionally, just as he had put the name Felix Dzerzhinsky in one; and that some files released by proxy in September were copied locally) were not that controversial and certainly don't refute the Intelligence Community conclusion that Russia was behind these hacks.

I also pointed out something that came out of that and related research – the understanding that the documents Guccifer 2.0 first released *weren't the DNC documents released to WikiLeaks at all*, and so had absolutely no bearing on the question of whether Guccifer 2.0 provided the DNC documents to WikiLeaks. The NYer's Raffi Khatchadourian used that same data as part of his argument that Russia was clearly working with WikiLeaks.

Cui bono from DCCC documents

Not only does all this analysis focus on the DNC when it really should focus on Hillary documents, but it almost entirely ignores the later documents Guccifer 2.0. For example, here's how Adam Carter dismisses the import of the DCCC documents in considering attribution.

The documents he posted online were a

mixture of some from the public domain (eg. already been published by OpenSecrets.org in 2009), were manipulated copies of research documents originally created by Lauren Dillon (see *attachments*) and others or were legitimate, unique documents that were of little significant damage to the DNC. (Such as the DCCC documents)

The DCCC documents didn't reveal anything particularly damaging. It did include a list of fundraisers/bundlers but that wasn't likely to cause controversy (the fundraising totals, etc. are likely to end up on sites like OpenSecrets, etc within a year anyway). – It did however trigger 4chan to investigate and a correlation was found between the DNC's best performing bundlers and ambassadorships. – This revelation though, is to be credited to 4chan. – The leaked financial data wasn't, in itself, damaging – and some of the key data will be disclosed publicly in future anyway.

Even ignoring that some of these documents provided the DCCC's views of races and candidates, the notion that data will one day become public in no way minimizes the value of having that data in time for an electoral race, which is what Guccifer 2.0's release of them did.

Even Khatchadourian simply nods at what, given the timing, are likely the DCCC documents. After laying out what are suggestions of pressure Assange's source is exerting on WikiLeaks in the early summer, he reveals that in August, Guccifer 2.0 considered leaking documents through Emma Best (who, notably, had just linked the Turkish emails that WikiLeaks would get blamed for at the end of July).

In mid-August, Guccifer 2.0 expressed interest in offering a trove of

Democratic e-mails to Emma Best, a journalist and a specialist in archival research, who is known for acquiring and publishing millions of declassified government documents. Assange, I was told, urged Best to decline, intimating that he was in contact with the persona's handlers, and that the material would have greater impact if he released it first.

Given the mid-August date, those emails are likely the DCCC emails that Guccifer 2.0 first announced on August 12 by publishing the contact information of members and their key staffers (one of the several things over the course of the operation that got suppressed by providers). While Khatchadourian doesn't dwell on what happened to them instead of release via Best, it is significant: Guccifer 2.0 reached out to local journalists to report on the state-level data. That is, for a limited set of what must have been available at DCCC, a set focused on swing states (which, contrary to what Carter suggests, cannot be bracketed off from the top of the ticket in a presidential year), Guccifer 2.0 worked to magnify these documents too, with mixed success.

It's hard to imagine why anyone associated with the Democratic party or CrowdStrike – who both have been accused of being the real insiders behind the Wikileaks documents – would release those documents, no matter how uninteresting people outside of politics find them. Likewise, even the most bitter Bernie supporter would have little reason to help Republicans get elected to Congress. Leaking boring but useful documents that benefit just Republicans doesn't even fit with the hacktivist persona Guccifer 2.0 presented as. That leaves GOPers, as well as the Russians if they were siding with the GOP, with sufficient motive to hack and leak them.

Moreover, given questions about whether Republicans incorporated data made available by Russia in their own data analysis, the release

of these documents may have provided a way to do that while maintaining plausible deniability. This stuff could get more interesting now, given that Ron DeSantis, who benefitted from these state level leaks, wants to cut the Mueller investigation short.

What about Guccifer 2.0's Clinton Foundation headfake?

Which brings us to some other still unexplained events from last year: Roger Stone's promises that WikiLeaks would release the Clinton Foundation emails in early October. A lot gets missed in the public narrative of that period. Stone turned out to repeatedly promise files, only to be wrong, which (on its face, anyway) undermines Democratic accusations he was in cahoots with WikiLeaks. And ultimately, WikiLeaks didn't publish the Clinton Foundation files; instead, it released the Podesta document that included excerpts of Hillary's speeches. Though – again, contrary to what the Democrats now complain – those were completely drowned out by the Access Hollywood release. No one mentions, either, that Stone sort of sulked away, uninterested in WikiLeaks emails anymore, moving on to Bill Clinton rape allegations. What happened?

Here's what I laid out in April.

CNN has a timeline of many of Stone's Wikileaks related comments, which actually shows that in August, at least, Stone believed Wikileaks would release Clinton Foundation emails (a claim that derived from other known sources, including Bill Binney's claim that the NSA should have all the Clinton Foundation emails).

It notes, as many timelines of Stone's claims do, that on Saturday October 1 (or early morning on October 2 in GMT;

the Twitter times in this post have been calculated off the unix time in the source code), Stone said that on Wednesday (October 5), Hillary Clinton is done.



Fewer of these timelines note that Wikileaks didn't release anything that Wednesday. It did, however, call out Guccifer 2.0's purported release of Clinton Foundation documents (though the documents were real, they were almost certainly mislabeled Democratic Party documents) on October 5. The fact that Guccifer 2.0 chose to mislabel those documents is worth further consideration, especially given public focus on the Foundation documents rather than other Democratic ones. I'll come back to that.

Throughout the week – both before and after the Guccifer 2.0 release – Stone kept tweeting that he trusted the Wikileaks dump was still coming.

Monday, October 3:



Wednesday, October 5 (though this would have been middle of the night ET):



Thursday, October 6 (again, this would have been nighttime ET, after it was clear Wikileaks had not released on Wednesday):



On October 7, at 4:03PM, David Fahrenthold tweeted out the Access Hollywood video.

On October 7, at 4:32 PM, Wikileaks started releasing the Podesta emails.

Stone didn't really comment on the substance of the Wikileaks release. In fact, even before the Access Hollywood release, he was accusing Bill Clinton of rape, and he continued in that vein after the release of the video, virtually ignoring the Podesta emails.

Two parts of this narrative now look very different, given what we know now. As noted, Kachadourian argues that Guccifer 2.0 served as a pressure point for WikiLeaks, pushing Assange to release things on the persona's timeline. I've long been puzzled (for obvious reasons) by Guccifer 2.0's response to my tweet, calling out his supposed October 4 release of Clinton Foundation documents as the bullshit it was.



There was no private conversation behind this – Guccifer 2.0 and I never spoke by DM. My guess is he chose to respond to my tweet because Glenn Greenwald immediately responded to me and took my debunking seriously, though Guccifer 2.0's response was quick – within 45 minutes. And only after that tweet did he follow me. It was a rare unsolicited response to someone, and it was one of maybe three tweets he sent responding to a criticism. (Interesting side note: I realized when reviewing his tweets that a few of Guccifer 2.0's tweets appear in Twitter's count but are not visible.) In other words, Guccifer 2.0 apparently wanted to respond to my debunking, perhaps because Greenwald found them credible, thereby sustaining the claim he really had Clinton Foundation emails. But it happened at a time when Stone, too, was pushing WikiLeaks to release Clinton Foundation emails.

Now couple that information with the details of GOP rat-fucker Peter Smith's attempt to hunt down Clinton Foundation emails. As Matt Tait describes, close to the July 22 release of the the DNC emails, Smith contacted him *already having been contacted* by someone who claimed to have copies of Hillary's Clinton Foundation emails.

Over the course of a long phone call, he mentioned that he had been contacted by someone on the "Dark Web" who claimed to have a copy of emails from Secretary Clinton's private server, and this was why he had contacted me; he wanted me to help validate whether or not the emails were genuine.

The WSJ explained that Smith could never authenticate any of the emails he got pitched, which is why they weren't ever published, and recommended they be dealt to WikiLeaks.

So what if someone actually *did* deal those emails to WikiLeaks, authentic or not? What if Guccifer 2.0 somehow knew that? It would explain Stone's certainty they'd come out, Guccifer 2.0's attempt to claim he had them, and the back-and-forth in early October.

Incidentally, the latest stink in the right wing noise machine is that a guy trying to obtain more Hillary related emails via FOIA got denied because the public interest doesn't outweigh Hillary's privacy interests. [Deleted: this was one of the fake Assange accounts—thanks to Arbed for heads up.] ~~Assange claim he has duplicates.~~

~~To be clear, I don't believe those are Clinton Foundation emails. But I find the possibility that Assange may still be getting and releasing materials damning to Hillary.~~

Guccifer 2.0's other propaganda

Finally, it's worth noting that these reassessments of Guccifer 2.0 largely look at the documents he released, out of context of the things he said.

I think that's particularly problematic given this last two posts, which align with activities alleged to have ties to Russia. His second-to-last post was typically nonsensical (the FEC's networks have nothing to do with vote counting). But it attributed any tampering with software to Democrats.

**INFO FROM INSIDE
THE FEC: THE**

DEMOCRATS MAY RIG THE ELECTIONS

I'd like to warn you that the Democrats may rig the elections on November 8. This may be possible because of the software installed in the FEC networks by the large IT companies.

As I've already said, their software is of poor quality, with many holes and vulnerabilities.

I have registered in the FEC electronic system as an independent election observer; so I will monitor that the elections are held honestly.

I also call on other hackers to join me, monitor the elections from inside and inform the U.S. society about the facts of electoral fraud.

We've since learned (most recently in this NYT piece) that there was more risk of tampering with the vote count than initially revealed. And no matter whether or not you believe the Russians did it, there is no credible reason why Democrats would target turnout that they needed to win the election. This message, Guccifer 2.0's last before the election, could only serve to give pre-emptive cover for any tampering that did get discovered.

Finally, there's Guccifer 2.0's last post, bizarrely posted months after he seemed to be done, capitalizing on legitimate complaints about the first Joint Analysis Report released on December 29 to suggest the evidence implicating him as Russian is fake.

The technical evidence contained in the reports doesn't stand up to scrutiny. This is a crude fake.

Any IT professional can see that a malware sample mentioned in the Joint Analysis Report was taken from the web

and was commonly available. A lot of hackers use it. I think it was inserted in the report to make it look a bit more plausible.

But several things are interesting about this post (in addition to the way it coincided with what Shadow Brokers claimed was going to be his last post). In spite of using the singular “this” to refer to the “reports,” Guccifer 2.0 claims that several reports tie him to Russia.

The U.S. intelligence agencies have published several reports of late claiming I have ties with Russia.

But the JAR actually doesn’t mention him at all. What does mention him is the Intelligence Community Assessment.

We assess with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets.

Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.

Guccifer 2.0’s silence about the ICA is all the more interesting given that the post – dated January 12 and so immediately after the leak of the Steele dossier – doesn’t mention that, but says the Obama Administration would release more fake information in the coming week.

Certainly, those who believe Guccifer 2.0 is not Russian even while noting his many false claims will take this post as gospel. But it’s worth

noting that it doesn't actually refute the substance of the claims made about Guccifer 2.0, rather than Russia.

Reassessing the Role of Guccifer 2.0 Should Not Terrify Analysts

I'm glad folks are still poking around the Guccifer 2.0 documents, and applaud the openness of the researchers to respond to criticism. Frankly, it's a model those who made initial claims about Guccifer 2.0 – most egregiously, that Cyrillic metadata in a document adopting the name of Felix Dzerzhinsky would not be every bit as intentional as that graffiti – should adopt. There were errors in the early analysis of the Guccifer 2.0 persona (such as the assumption he was publishing DNC documents), that, with hindsight, are more clear. One particularly annoying one is the logic that because Guccifer 2.0 got caught pretending to be Romanian – a claim he backed off of in his FAQ a week later in any case – he had to be Russian. The unwillingness to revise early analysis only feeds the distrust of the Russian attribution.

That said, in my opinion nothing about the new analysis undermines the claim of Russian attribution, and the majority of the known evidence does support it (and has since been backed – for example – by Facebook, which has its own set of global data to draw from).

Update: I thought Stone was involved in the Smith effort. This article describes him as chatting to Guccifer 2.0 at the direction of Smith.

“The magnitude of what he was trying to do was kind of impressive,” Johnson said. “He had people running around Europe, had people talking to Guccifer.” (U.S. intelligence agencies have linked the materials provided by “Guccifer 2.0”—an alias that has taken credit for

hacking the Democratic National Committee and communicated with Republican operatives, including Trump confidant Roger Stone—to Russian government hackers.)