WITHOUT INTEGRITY: THE DEBUNKING OF THE METADATA DEBUNKERS

As I laid out a few weeks ago, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.

When people have asked me if I've gotten a lot of pushback since I revealed that I provided information to the FBI on a matter that became part of the Mueller inquiry, I've said that I'm mostly surprised by how little I've gotten. While I've had a few alarms with respect to my website or device security (which I might attribute to Russians), I've had almost no pushback from Republicans accusing me of gunning for the President, not even after I suggested my testimony probably changed the import of publicly available information that implicated the President.

The exception has been a group of Assange loyalists close to Adam Carter – a group of people who have spent a great deal of time trying to undermine the public case implicating Russia in the attack. I have been shocked by the persistence with which Carter loyalists flooded my timeline at certain times in recent weeks, even though nothing I've said publicly would indicate Carter's efforts were put in any great danger because I went to the FBI sometime last year.

Today, Duncan Campbell released a long story on the guy behind the pseudonym Adam Carter, Tim Leonard.

Before I look at it, two comments. First, contrary to some guesses, Leonard is not the person I went to the FBI about. Second, I think

there are still details in this story that are not correct (though are far closer than other work thus far); one value of Leonard's effort was to get some people (including me!) to work through assumptions, something people are still not doing enough on this story.

Campbell's is an important and successful effort to push back against disinformation (and to get Bill Binney and Ray McGovern to back off their support for it). It does the following:

- Affirmatively IDs Leonard, demonstrates that he used the facilities of his employer to do some of this work, and shows how he falsely blamed a former co-worker for some of the work
- Shows how Leonard serially adopted ever new theories, but never the one almost every expert had backed, that Russia had done the hack
- Shows the co-travelers, including the far right, that Leonard embraced in his efforts to discredit the dominant explanation
- Tracks some of the false identities Leonard adopted along the way (I believe, given the data in the story, he has adopted false IDs on this site as well)

This work is particularly valuable because it demonstrates how early – by May 2016 – Leonard focused attacks on Clinton before coming out with his debunking site.

> As US election campaigns ramped up in May 2016, Leonard's Defianet email address, op@d3f.uk, was used to create a new Twitter account, @with_integrity. The name, he said, was a parody of Clinton's campaign slogan, "I'm with Hillary". The profile displayed a WikiLeaks avatar.
>
> For 10 days in 2016, @with_integrity trolled and attacked the Democratic Convention, accusing the Democrats of collusion, conspiracy, cheating, corruption, rigging elections and sabotage.
>
> On 22 July 2016, @with_integrity tweeted a link to the Russian propaganda and news channel, RT, claiming that primary elections had been rigged. On 26 July, as delegates voted, @with_integrity tweeted a new RT attack on Hillary Clinton.
>
> After Clinton was nominated, @with_integrity followed the Russian trolls' path in supporting Donald Trump, retweeting Trump slogans, including #CrookedHillary, #LockHerUp, #MakeAmericaGreatAgain and #VoteOnlyTrump, and a third link to a "special episode" on RT.

But the core of Campbell's debunking (and the basis of his success at persuading Binney and McGovern, to the extent he did) pertains to the Forensicator effort to claim that certain files released in September 2016 proved that Russia couldn't have done the hack because they had been copied in the Eastern time zone. Campbell shows that shows that the data behind the Forensicator effort had been adopted uncritically by Leonard and his allies, and that the most obvious conclusion based on the evidence is that hackers manipulated the timestamps of these files, and only these files.

> The team that created Forensicator, including Leonard, gave away that they were not the real authors of the analysis when they inaccurately copied a Linux “Bash” script they had been sent, breaking it. This suggested that they did not write, understand, or test the script before they published. Someone else had sent the script, together with the fake conclusion they wanted discovered and published – that DNC stolen files had been copied in the US Eastern Time zone on 5 July 2016, five days before DNC employee Seth Rich was killed.
>
> Uncritical reporters failed to spot that the Forensicator blog gave no evidence for its conclusion, which was that the data analysed was evidence of theft by local copying happening within the eastern US. The Forensicator report avoided pointing out that the time stamps examined were present only in the special London group of documents, and not in tens of thousands of other DNC files published by WikiLeaks or Guccifer 2.0.
>
> The files were manipulated using an unusual method of file packing, forensic checks show. Because of computer clock settings, the packing operations appeared to have created “evidence” that the stolen files had been copied in the US Eastern Time zone, which includes Washington.
>
> US Eastern Standard Time (EST) is normally five hours behind Coordinated Universal Time (UTC) – better known in Britain as Greenwich Mean Time (GMT). In summer months, clocks are set forward, placing the US Eastern Daylight Time (EDT) four hours behind UTC. The difference between a time zone and UTC is the offset. It is trivially easy for

> any computer user to change their time, date and time zone offset, using standard controls.
>
> The files released in London, we found, had first been processed in this way to show timestamps for 5 July 2016. Some 13 groups had then been compressed using WinRAR 4.2. Nine additional files were compressed using 7zip. The archive, called 7dc58-ngp-van.7z, was published in this format, as a single file of 680MB.
>
> This dual compression method was unique to the London documents. It was not used in other file dumps released by Guccifer 2.0, WikiLeaks or other publishers of stolen DNC material. The special method used two different file compression systems, 7zip and WinRAR, and required using a four-year-old, superseded version of WinRAR to obtain the required result. The way the Russians did it, the two compression operations appeared to overlap within a single 20-minute period. The tampering may have been done on 1 September, a week before the London conference.
>
> [snip]
>
> The obvious, simple explanation was that hackers were manipulating computer clock settings. The observed changes would have taken seconds.

In response to Campbell's piece, Leonard has complained that Campbell doxed him rather than debunk the evidence.

> He doesn't actually tackle what he's framing as disinformation and instead tries to attack character and tries to dox people rather than discredit or debunk the evidence/research published. You don't tackle disinfo with smears/distortion/character attacks yet

> this is what DC did.

This is where I get a little cranky — probably crankier than I otherwise would have been if Leonards fans hadn't flooded my timelines in recent weeks.

Campbell is actually wrong when he claims that "uncritical reporters" didn't point out that this file was a unique file. I noted this file was a proxy file back in October, and that before you got into the analysis of its forensics, you first had to account for the provenance of it. I also noted WikiLeaks' role in sharing the file with the Trump campaign here. In this post, I noted that the files in question weren't DNC files (nor were the earliest Guccifer 2.0 ones), so the entire exercise said absolutely nothing about who hacked the DNC, purportedly the central project of Leonard and his ilk. And all that's before I noted, over and over, that copying of files in the US would not prove a damn thing (as the GRU's use of staging servers in AZ and IL make clear).

I raise these posts not to challenge Campbell's reporting, but instead to challenge Leonard's complaint. He has claimed for over a year now that he would respond to legitimate responses to his theories. And while I vaguely recall him making a half-hearted attempt at it on his site, I can't find it.

Even before you get into the evidence of a concerted disinformation campaign — one that paralleled if it wasn't coordinated with at least WikiLeaks if not the Russians' — you've got to be arguing facts that might address the questions you claim to. And Leonard quickly strayed from that purported effort, never to return again.