

Hack or Leak: Who Really Stole the DNC Files?

Lack of forensics leads to muddy waters indeed.

By [Philip Giraldi](#)

Global Research, August 15, 2017

[The American Conservative](#)

Region: [Russia and FSU](#), [USA](#)

Theme: [Intelligence](#), [Media Disinformation](#)

In-depth Report: [FAKE INTELLIGENCE](#), [U.S. Elections](#)

Congress and Special Counsel Robert Mueller are looking into whether there was Donald Trump campaign collusion with the Russian government to “influence” the results of the 2016 presidential election. Stupidity and naivete will probably be revealed in abundance, but collusion to alter the outcome of an election—and thereby damage American democracy—is unlikely to be demonstrated.

The mantra in Washington, both within the media and the inside-the-beltway establishment, is that Russia actively “interfered” in the election and may have changed the outcome, but that is largely speculative. Since the line between possibly influencing or favoring a certain outcome and interfering has been rather difficult to discern, Russiagate has evolved into a seemingly never-ending inquiry that will likely produce nothing in terms of indictable criminality among the Trumpsters. The Russians for their part will likely be seen to have engaged important individuals in a foreign country to advance their own interests—something governments worldwide do.

Indeed, the process itself seems to be backwards. Unlikely to be revealed is how the whole affair became a national-security issue in the first place. Who exactly stole the files from the DNC server and the emails from John Podesta? It would seem to me that appreciating how the theft of the documents took place is crucial to understanding what has come to be called Russiagate. Demonstrate exactly what occurred and many of the other pieces will inevitably fall into place.

At this point, all that is clearly known after more than a year of huffing and puffing is that last summer files and emails pertaining to the election were copied and then made their way to WikiLeaks, which published some of them at a time that was damaging to the Clinton campaign. Those who are blaming Russia believe that there was a hack of the Democratic National Committee (DNC) server and also of John Podesta’s emails that was carried out by a Russian surrogate or directly by Moscow’s military intelligence arm. They base their conclusion on [a statement](#) issued by the Department of Homeland Security on October 7, 2016, and on a [longer assessment](#) prepared by the Office of the Director of National Intelligence on January 6.

Both government appraisals implied that there was a U.S. government intelligence agency consensus that there was a Russian hack, though they provided little in the way of actual evidence that that was the case and, in particular, failed to demonstrate how the information was obtained and what the chain of custody was as it moved from that point to the office of WikiLeaks. The January report was particularly criticized as unconvincing, rightly

so, because the most important one of its three key contributors, the National Security Agency, had only moderate confidence in its conclusions, suggesting that whatever evidence existed was far from solid.

Leaked reporting in the mainstream media subsequently [provided some clues](#) regarding what was behind the alleged intelligence community judgement. A hacker identified as Guccifer 2 might have broken into the system on behalf of Russia and there were reportedly traces of electronic fingerprints in the alleged intrusion that were characteristic of Russian intelligence hacks. Both of those assertions have been separately challenged and it has been observed that they are somewhat speculative. There are also reports that [intercepted Kremlin phone conversations](#) involving high level officials expressed considerable joy at the Trump victory, suggesting that Moscow was closely monitoring and possibly playing some role in the electoral process.

An alternative view that has been circulating for months suggests that it was not a hack at all, that it was a deliberate [whistleblower-style leak](#) of information carried out by as yet unknown parties that may have been provided to WikiLeaks for possible political reasons, perhaps to express disgust with the DNC manipulation of the nominating process to favor Hillary Clinton.

There are, of course, still other equally non-mainstream explanations for how the bundle of information got from point A to point B, including that the intrusion into the DNC server was [carried out by the CIA](#), which then made it look like it had been the Russians as perpetrators. That explanation has some plausibility due to the fact that the agency does indeed have cyber-capability to do just that when it goes around the globe and invades foreign information systems. It could also have easily come up with a credible role player who might have pretended that the information came from a dissident Democrat for passage to Assange.

And then there is the hybrid point of view, which is essentially that the Russians or a surrogate did indeed intrude into the DNC computers but it was all part of normal intelligence agency probing and did not lead to anything. Meanwhile and independently, someone else who had access to the server was downloading the information, which in some fashion made its way from there to WikiLeaks.

Both the hack vs. leak viewpoints have marshalled considerable technical analysis in the media to bolster their arguments. The hack school of thought has stressed that Russia had both the ability and motive to interfere in the election by exposing the stolen material while the leakers have recently asserted that the [sheer volume of material](#) downloaded indicates that something like a higher speed thumb drive was used, meaning that it had to be done by someone with actual physical direct access to the DNC system.

What the many commentators on the DNC server issue choose to conclude is frequently shaped by their own broader political views, producing a result that favors one approach over another depending on how one feels about Trump or Clinton. Perhaps it would be clarifying to regard the information obtained and transferred as a theft rather than either a hack or a leak, since the two expressions have taken on a political meaning of their own in the context of Russiagate. I am not qualified to judge the technical analyses that have been done on the theft, but I would like to suggest that the bottom line is that we (the American people and government) have no idea who actually stole the material in question.

If Congress were seriously interested in determining who did what to whom, it would have started with the theft of the information. The inquiry should have begun with the DNC server or servers where the information that was stolen was stored, but, oddly, the FBI was [not allowed access](#). So whatever forensic insights that might have been obtained from the actual computers has never been collected or developed by federal law enforcement, which perforce relied instead on an assessment made by a DNC contractor, CrowdStrike, whose co-founder Dmitri Alperovitch is a prominent critic of the Russian government. CrowdStrike ran [its own investigation](#) and inevitably blamed the Russians.

If the FBI had moved quickly to do a forensic examination on the computers, information retained in the system presumably could have told investigators exactly who logged in and at what times. With that in hand, questioning of the individuals identified could have begun. Also, a thorough investigation would include obtaining a list of all those individuals who theoretically had access to the information that was stolen under the assumption that someone might have been using an associate's password. Yet there is no indication that any questioning of those with access to the DNC system has occurred or is even being contemplated.

A good investigation would also examine possible motive. Back in July there was little doubt that Hillary Clinton would win the election and it is far-fetched to think that the Russians would in even their wildest imaginings think that they could change the result. But that is not to say that they would not have been interested in weakening the Clinton presidency by surfacing evidence of a scandal. Nor is there any motive for then CIA Director John Brennan to do a hack and blame it on Moscow since he would have known that the information being released would damage his candidate, Hillary Clinton—but he might have thought that promoting the Russian connection would do even worse damage to Trump. It seems to me that likely motive also includes two other plausible possibilities: that someone took the information to sell it to a party who has not yet been identified, or that someone stole the information to get even either with the Democratic establishment or with individuals running the primaries and the convention.

As there would have been only a [limited market](#) for the Clinton papers and their sale would be tricky and require developing contacts desirous of obtaining such information, revenge would seem to be the more likely explanation. But even there we know nothing as no names have surfaced as part of whatever has been passing for an investigation. DNC staffer [Seth Rich](#), who was killed in a still unexplained "robbery attempt" in Washington on July 10, 2016, has been identified as a potential suspect [by conservative media](#), but that possibility has been strenuously rejected by his family and others, and it does not appear that there has been any FBI follow-up on his case.

I honestly believe that we the public will never know who stole the Clinton and Podesta emails unless Julian Assange of WikiLeaks chooses to come clean on the issue, which is unlikely. In fact, Assange, who has denied that it was the Russians, might not know whom he was dealing with. If a sophisticated intelligence agency was somehow involved it could have used its own recruited assets as interlocutors, pretending to be who they were not. A well-constructed cover story could have easily fooled Assange. A capable spy agency would also have run its operation replete with red herrings while using cut-outs to break the transmission belt of the information so the theft could not plausibly be traced back to it, or to its sponsoring government.

The fact that more than a year of inquiry has gone by without anyone inside the DNC IT

system being investigated suggests that whatever happened has been buried so deep that it will never surface. Even now, it might pay some dividends for the FBI to examine the DNC server, but there is [virtually no pressure](#) from anyone to make that happen. Certainly the FBI has given no indication that it has a clue about what took place and is content with attributing it to the Russians, particularly since that seems to be the conventional wisdom. Blaming the theft and what happened subsequently on Moscow is both convenient and comforting because no American constituency gets offended and it means you don't really have to annoy anyone but Vladimir Putin.

Philip Girdali, a former CIA officer, is executive director of the Council for the National Interest.

Featured image is from [Shutterstock/cunaplus](#).

The original source of this article is [The American Conservative](#)
Copyright © [Philip Girdali](#), [The American Conservative](#), 2017

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Philip Girdali](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca