# More Holes in Russia-gate Narrative

**Exclusive:** New tests support the skepticism of U.S. intelligence veterans that Russia "hacked" the DNC's computers, pointing instead to a download of emails by an insider, write ex-NSA official William Binney and ex-CIA analyst Ray McGovern.

By William Binney and Ray McGovern

It is no secret that our July 24 VIPS Memorandum for the President, entitled "Was the 'Russian Hack' an Inside Job?," gave rise to some questioning and controversy – nor was it a surprise that it was met with almost total silence in the mainstream media.

The ongoing U.S. media campaign against Russia has been so effective that otherwise intelligent people have been unable even to entertain the notion that they may have been totally misled by the intelligence community. The last time this happened in 2003, after a year of such propaganda, the U.S. attacked Iraq on fraudulent – not "mistaken" – intelligence.

Anticipating resistance from those allergic to rethinking "what everybody knows" about Russian "meddling," we based our VIPS analysis on forensic investigations that, oddly, the FBI had bent over backwards to avoid. In other words, we relied on the principles of physics and the known capability of the Internet in early July 2016.

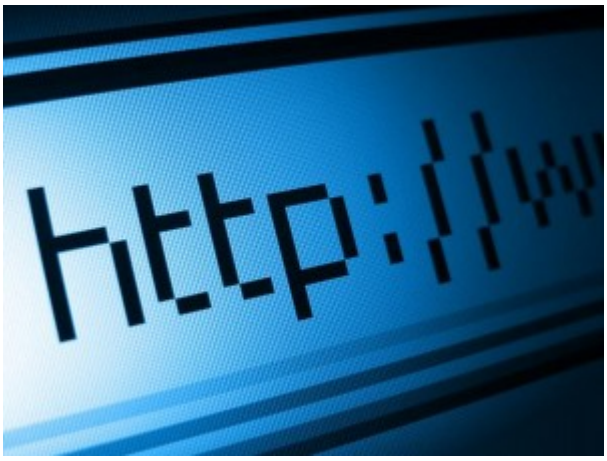
We stand by our main conclusion that the data from the intrusion of July 5, 2016, into the Democratic National Committee's computers, an intrusion blamed on "Russian hacking," was not a hack but rather a download/copy onto an external storage device by someone with physical access to the DNC.

That principal finding relied heavily on the speed with which the copy took place – a speed much faster than a hack over the Internet could have achieved at the time – or, it seems clear, even now. Challenged on that conclusion – often by those conducting experiments within the confines of a laboratory – we have conducted and documented additional tests to determine the speeds that can be achieved now, more than a year later.

To remind: We noted in the VIPS memo that on July 5, 2016, a computer directly connected to the DNC server or DNC Local Area Network, copied 1,976 megabytes of data in 87 seconds onto an external storage device. That yields a transfer rate of ***22.7 megabytes per second.***

**Recent Tests**

Over the last few weeks, we ran three tests to determine how quickly data could be exfiltrated from the U.S. across the Atlantic to Europe.




–First, we used a 100 megabits-per-second (mbps) line to pull data from a one-gigabyte file to Amsterdam. The peak transfer speed was **.8 MBps.**

–Second, we used a commercial DSL (Digital Subscriber Line) to send the same one-gigabyte file to a commercial DSL in Amsterdam. The peak transfer speed was **1.8 MBps.**

–Third, we pushed the same one-gigabyte file from a data center in New Jersey to a data center in the UK. The peak transfer speed was **12 MBps.**

None of these attempts achieve anything close to the average rate of **22.7 megabytes per second** evident in the July 5, 2016 download/copy associated with the DNC. In fact, this happens to be the speed typical of a transfer to a USB-2 external storage device. We do not think this pure coincidence; rather, it is additional evidence of a local download.

We are preparing further trans-Atlantic testing over the next few weeks.

Some researchers have noted that some partitioning of the data might have occurred in the U.S., allowing for a transfer to be made at the measured speed over the Internet, and that this could have made possible a hack from the other side of the Atlantic. One of our associate investigators has found a way to achieve this kind of data partitioning and later transfer.

In theory, this would be one possible way to achieve such a large-data transfer, but we have no evidence that anything like this actually occurred. More important, in such a scenario, the National Security Agency would have chapter and verse on it, because such a hack would have to include software to execute the partitioning and subsequent data transfer. NSA gives the highest priority to collection on “execution software.”

Must Americans, apparently including President Donald Trump, remain in a Russia-did-it-or-could-have-maybe-might-have-done-it subjunctive mood on this important issue – one that has been used to inject Cold War ice into relations with Russia? The answer is absolutely not. Rather, definitive answers are at hand.

How can we be so confident? Because NSA alumni now active in Veteran Intelligence Professionals for Sanity (VIPS) are intimately familiar with NSA's capabilities and practice with respect to bulk capture and storage of fiber-optic communications. Two of us actually devised the systems still in use, and Edward Snowden's revelations filled in remaining gaps. Today's NSA is in position to clear up any and all questions about intrusions into the DNC.

In sum, we are certain that the truth of what actually happened – or didn't happen – can be found in the databases of NSA. We tried to explain this to President Barack Obama in a VIPS Memorandum of Jan. 17, just three days before he left office, noting that NSA's known programs are fully capable of capturing – and together with liaison intelligence services do capture – all electronic transfers of data.

Our Jan. 17 Memorandum included this admonition: "We strongly suggest that you ask NSA for any evidence it may have indicating that the results of Russian hacking were given to WikiLeaks." … "If NSA cannot give you that information – and quickly – this would probably mean it does not have any."

We also appealed to Obama in his final days in office to order the chiefs of the NSA, FBI and CIA to the White House and have them lay all their cards on the table about "Russian hacking," and show him what tangible evidence they might have – not simply their "assessments." We added, "We assume you would not wish to hobble your successor with charges that cannot withstand close scrutiny." Having said this, we already were reaching the assumption that there was no real evidence to back the "assessments" up.

**FBI: Not Leaning Forward**

The FBI could still redeem itself by doing what it should have done as soon as the DNC claimed to have been "hacked." For reasons best known to former FBI Director James Comey, the Bureau failed to get whatever warrant was needed to confiscate the DNC servers and computers to properly examine them.

In testimony to the House Intelligence Committee six months ago, Comey conceded "best practice is always to get access to the machines themselves." And yet he chose not to. And his decision came amid frenzied charges by senior U.S. officials that Russia had committed "an act of war."

But is it not already too late for such an investigation? We hope that, at this

point, it is crystal clear that the answer is: No, it is not too late. All the data the FBI needs to do a proper job is ***in NSA databases*** – including data going across the Internet to the DNC server and then included in their network logs.

If President Trump wants to know the truth, he can order the FBI to do its job and NSA to cooperate. Whether the two and the CIA would obey such orders is an open question, given how heavily invested all three agencies are in their evidence-impoverished narrative about "Russian hacking."

Let us close with the obvious. All three agencies have been aware all along that NSA has the data. One wonders why it should require a Presidential order for them to delve into that data and come up with conclusions based on fact, as opposed to "assessing."

**William Binney (williambinney0802@comcast.net) worked for NSA for 36 years, retiring in 2001 as the technical director of world military and geopolitical analysis and reporting; he created many of the collection systems still used by NSA. Ray McGovern (rrmcgovern@gmail.com) was a CIA analyst for 27 years; from 1981 to 1985 he briefed the *President's Daily Brief* one-on-one to President Reagan's most senior national security officials.**