Intel Vets Challenge ‘Russia Hack’ Evidence

In a memo to President Trump, a group of former U.S. intelligence officers, including NSA specialists, cite new forensic studies to challenge the claim of the key Jan. 6 “assessment” that Russia “hacked” Democratic emails last year.

MEMORANDUM FOR: The President

FROM: Veteran Intelligence Professionals for Sanity (VIPS)

SUBJECT: Was the “Russian Hack” an Inside Job?

Executive Summary

Forensic studies of “Russian hacking” into Democratic National Committee computers last year reveal that on July 5, 2016, data was ***leaked (not hacked)*** by a person with physical access to DNC computer. After examining metadata from the “Guccifer 2.0” July 5, 2016 intrusion into the DNC server, independent cyber investigators have concluded that an insider copied DNC data onto an external storage device.

Key among the findings of the independent forensic investigations is the conclusion that the DNC data was copied onto a storage device ***at a speed that far exceeds an Internet capability for a remote hack***. Of equal importance, the forensics show that the copying was performed on the East coast of the U.S. Thus far, mainstream media have ignored the findings of these independent studies [see here and here].

Independent analyst Skip Folden, who retired after 25 years as the IBM Program Manager for Information Technology, US, who examined the recent forensic findings, is a co-author of this Memorandum. He has drafted a more detailed technical report titled “Cyber-Forensic Investigation of ‘Russian Hack’ and Missing Intelligence Community Disclaimers,” and sent it to the offices of the Special Counsel and the Attorney General. VIPS member William Binney, a former Technical Director at the National Security Agency, and other senior NSA “alumni” in VIPS attest to the professionalism of the independent forensic findings.

The recent forensic studies fill in a critical gap. Why the FBI neglected to perform any independent forensics on the original “Guccifer 2.0” material remains a mystery – as does the lack of any sign that the “hand-picked analysts” from the FBI, CIA, and NSA, who wrote the “Intelligence Community Assessment”

dated January 6, 2017, gave any attention to forensics.

NOTE: There has been so much conflation of charges about hacking that we wish to make very clear the primary focus of this Memorandum. We focus specifically on the July 5, 2016 alleged Guccifer 2.0 "hack" of the DNC server. In earlier VIPS memoranda we addressed the lack of any evidence connecting the Guccifer 2.0 alleged hacks and WikiLeaks, and we asked President Obama specifically to disclose any evidence that WikiLeaks received DNC data from the Russians [see here and here].

Addressing this point at his last press conference (January 18), he described "the conclusions of the intelligence community" as "not conclusive," even though the Intelligence Community Assessment of January 6 expressed "high confidence" that Russian intelligence "relayed material it acquired from the DNC … to WikiLeaks."

Obama's admission came as no surprise to us. It has long been clear to us that the reason the U.S. government lacks conclusive evidence of a transfer of a "Russian hack" to WikiLeaks is because there was no such transfer. Based mostly on the cumulatively unique technical experience of our ex-NSA colleagues, we have been saying for almost a year that the DNC data reached WikiLeaks via a copy/leak by a DNC insider (but almost certainly not the same person who copied DNC data on July 5, 2016).

From the information available, we conclude that the same inside-DNC, copy/leak *process* was used at two different times, by two different entities, for two distinctly different purposes:

-(1) an inside leak to WikiLeaks before Julian Assange announced on June 12, 2016, that he had DNC documents and planned to publish them (which he did on July 22) – the presumed objective being to expose strong DNC bias toward the Clinton candidacy; and

-(2) a separate leak on July 5, 2016, to pre-emptively taint anything WikiLeaks might later publish by "showing" it came from a "Russian hack."

* * *

Mr. President:

This is our first VIPS Memorandum for you, but we have a history of letting U.S. Presidents know when we think our former intelligence colleagues have gotten something important wrong, and why. For example, our first such memorandum, a same-day commentary for President George W. Bush on Colin Powell's U.N. speech on February 5, 2003, warned that the "unintended consequences were likely to be

catastrophic," should the U.S. attack Iraq and "justify" the war on intelligence that we retired intelligence officers could readily see as fraudulent and driven by a war agenda.

The January 6 "Intelligence Community Assessment" by "hand-picked" analysts from the FBI, CIA, and NSA seems to fit into the same agenda-driven category. It is largely based on an "assessment," not supported by any apparent evidence, that a shadowy entity with the moniker "Guccifer 2.0" hacked the DNC on behalf of Russian intelligence and gave DNC emails to WikiLeaks.

The recent forensic findings mentioned above have put a huge dent in that assessment and cast serious doubt on the underpinnings of the extraordinarily successful campaign to blame the Russian government for hacking. The pundits and politicians who have led the charge against Russian "meddling" in the U.S. election can be expected to try to cast doubt on the forensic findings, if they ever do bubble up into the mainstream media. But the technical limitations of today's Internet are widely understood. We are prepared to answer any substantive challenges on their merits.

You may wish to ask CIA Director Mike Pompeo what he knows about this. Our own lengthy intelligence community experience suggests that it is possible that neither former CIA Director John Brennan, nor the cyber-warriors who worked for him, have been completely candid with their new director regarding how this all went down.

Copied, Not Hacked

As indicated above, the independent forensic work just completed focused on data *copied (not hacked)* by a shadowy persona named "Guccifer 2.0." The forensics reflect what seems to have been a desperate effort to "blame the Russians" for publishing highly embarrassing DNC emails three days before the Democratic convention last July. Since the content of the DNC emails reeked of pro-Clinton bias, her campaign saw an overriding need to divert attention from content to provenance – as in, who "hacked" those DNC emails? The campaign was enthusiastically supported by compliant "mainstream" media; they are still on a roll.

"The Russians" were the ideal culprit. And, after WikiLeaks editor Julian Assange announced on June 12, 2016, "We have emails related to Hillary Clinton which are pending publication," her campaign had more than a month before the convention to insert its own "forensic facts" and prime the media pump to put the blame on "Russian meddling." Mrs. Clinton's PR chief Jennifer Palmieri has explained how she used golf carts to make the rounds at the convention. She wrote that her "mission was to get the press to focus on something even we found

difficult to process: the prospect that Russia had not only hacked and stolen emails from the DNC, but that it had done so to help Donald Trump and hurt Hillary Clinton."

Independent cyber-investigators have now completed the kind of forensic work that the intelligence assessment did not do. Oddly, the "hand-picked" intelligence analysts contented themselves with "assessing" this and "assessing" that. In contrast, the investigators dug deep and came up with verifiable evidence from metadata found in the record of the alleged Russian hack.

They found that the purported "hack" of the DNC by Guccifer 2.0 was not a hack, by Russia or anyone else. Rather it originated with a copy (onto an external storage device – a thumb drive, for example) by an insider. The data was leaked to implicate Russia. We do not know who or what the murky Guccifer 2.0 is. You may wish to ask the FBI.

The Time Sequence

June 12, 2016: Assange announces WikiLeaks is about to publish "emails related to Hillary Clinton."

June 14, 2016: DNC contractor Crowdstrike, (with a dubious professional record and multiple conflicts of interest) announces that malware has been found on the DNC server and claims there is evidence it was injected by Russians.

June 15, 2016: "Guccifer 2.0" affirms the DNC statement; claims responsibility for the "hack;" claims to be a WikiLeaks source; and posts a document that the forensics show was synthetically tainted with "Russian fingerprints."

We do not think that the June 12, 14, & 15 timing was pure coincidence. Rather, it suggests the start of a pre-emptive move to associate Russia with anything WikiLeaks might have been about to publish and to "show" that it came from a Russian hack.

The Key Event

July 5, 2016: In the early evening, Eastern Daylight Time, someone working in the EDT time zone with 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 speed is much faster than what is physically possible with a hack.***

It thus appears that the purported "hack" of the DNC by Guccifer 2.0 (the self-proclaimed WikiLeaks source) was not a hack by Russia or anyone else, but was rather a copy of DNC data onto an external storage device.

‘Obfuscation & De-obfuscation’

Mr. President, the disclosure described below may be related. Even if it is not, it is something we think you should be made aware of in this general connection. On March 7, 2017, WikiLeaks began to publish a trove of original CIA documents that WikiLeaks labeled “Vault 7.” WikiLeaks said it got the trove from a current or former CIA contractor and described it as comparable in scale and significance to the information Edward Snowden gave to reporters in 2013.

No one has challenged the authenticity of the original documents of Vault 7, which disclosed a vast array of cyber warfare tools developed, probably with help from NSA, by CIA’s Engineering Development Group. That Group was part of the sprawling CIA Directorate of Digital Innovation – a growth industry established by John Brennan in 2015.

Scarcely imaginable digital tools – that can take control of your car and make it race over 100 mph, for example, or can enable remote spying through a TV – were described and duly reported in the New York Times and other media throughout March. But the Vault 7, part 3 release on March 31 that exposed the “Marble Framework” program apparently was judged too delicate to qualify as “news fit to print” and was kept out of the Times.

The Washington Post’s Ellen Nakashima, it seems, “did not get the memo” in time. Her March 31 article bore the catching (and accurate) headline: “**WikiLeaks’ latest release of CIA cyber-tools could blow the cover on agency hacking operations.”**

The WikiLeaks release indicated that Marble was designed for flexible and easy-to-use “obfuscation,” and that Marble source code includes a “deobfuscator” to reverse CIA text obfuscation.

More important, the CIA reportedly used Marble during 2016. In her Washington Post report, Nakashima left that out, but did include another significant point made by WikiLeaks; namely, that the obfuscation tool could be used to conduct a “forensic attribution double game” or false-flag operation because it included test samples in Chinese, Russian, Korean, Arabic and Farsi.

The CIA’s reaction was neuralgic. Director Mike Pompeo lashed out two weeks later, calling Assange and his associates “demons,” and insisting; “It’s time to call out WikiLeaks for what it really is, a non-state hostile intelligence service, often abetted by state actors like Russia.”

Mr. President, we do not know if CIA’s Marble Framework, or tools like it, played some kind of role in the campaign to blame Russia for hacking the DNC. Nor do we know how candid the denizens of CIA’s Digital Innovation

Directorate have been with you and with Director Pompeo. These are areas that might profit from early White House review.

Putin and the Technology

We also do not know if you have discussed cyber issues in any detail with President Putin. In his interview with NBC's Megyn Kelly, he seemed quite willing – perhaps even eager – to address issues related to the kind of cyber tools revealed in the Vault 7 disclosures, if only to indicate he has been briefed on them. Putin pointed out that today's technology enables hacking to be "masked and camouflaged to an extent that no one can understand the origin" [of the hack] … And, vice versa, it is possible to set up any entity or any individual that everyone will think that they are the exact source of that attack."

"Hackers may be anywhere," he said. "There may be hackers, by the way, in the United States who very craftily and professionally passed the buck to Russia. Can't you imagine such a scenario? … I can."

Full Disclosure: Over recent decades the ethos of our intelligence profession has eroded in the public mind to the point that agenda-free analysis is deemed well nigh impossible. Thus, we add this disclaimer, which applies to everything we in VIPS say and do: We have no political agenda; our sole purpose is to spread truth around and, when necessary, hold to account our former intelligence colleagues.

We speak and write without fear or favor. Consequently, any resemblance between what we say and what presidents, politicians and pundits say is purely coincidental. The fact we find it is necessary to include that reminder speaks volumes about these highly politicized times. This is our 50th VIPS Memorandum since the afternoon of Powell's speech at the UN. Live links to the 49 past memos can be found at https://consortiumnews.com/vips-memos/.

FOR THE STEERING GROUP, VETERAN INTELLIGENCE PROFESSIONALS FOR SANITY

William Binney, former NSA Technical Director for World Geopolitical & Military Analysis; Co-founder of NSA's Signals Intelligence Automation Research Center

Skip Folden, independent analyst, retired IBM Program Manager for Information Technology US (Associate VIPS)

Matthew Hoh, former Capt., USMC, Iraq & Foreign Service Officer, Afghanistan (associate VIPS)

Larry C Johnson, CIA & State Department (ret.)

Michael S. Kearns, Air Force Intelligence Officer (Ret.), Master SERE Resistance to Interrogation Instructor

John Kiriakou, Former CIA Counterterrorism Officer and former Senior Investigator, Senate Foreign Relations Committee

Linda Lewis, WMD preparedness policy analyst, USDA (ret.)

Lisa Ling, TSgt USAF (ret.) (associate VIPS)

Edward Loomis, Jr., former NSA Technical Director for the Office of Signals Processing

David MacMichael, National Intelligence Council (ret.)

Ray McGovern, former U.S. Army Infantry/Intelligence officer and CIA analyst

Elizabeth Murray, former Deputy National Intelligence Officer for Middle East, CIA

Coleen Rowley, FBI Special Agent and former Minneapolis Division Legal Counsel (ret.)

Cian Westmoreland, former USAF Radio Frequency Transmission Systems Technician and Unmanned Aircraft Systems whistleblower (Associate VIPS)

Kirk Wiebe, former Senior Analyst, SIGINT Automation Research Center, NSA

Sarah G. Wilton, Intelligence Officer, DIA (ret.); Commander, US Naval Reserve (ret.)

Ann Wright, U.S. Army Reserve Colonel (ret) and former U.S. Diplomat

Editor's Note: This VIPS Memo included two mistaken dates. Neither affected the Memo's main conclusion; i.e., that the July 5, 2016 intrusion into DNC emails that was blamed on Russia could not have been a hack – by Russia or anyone else. The portions of the Memo affected by the mistaken dates have been corrected.

A short explanation of the corrections:

-(1) June 14, 2016 (not the 15th, as the VIPS memo erroneously stated) was the day Crowdstrike said malware had been found on the DNC server and claimed there was evidence the malware was injected by Russians. (On the following day – the 15th) – "Guccifer 2.0" claimed responsibility for the "hack" and claimed to be a WikiLeaks source.)

-(2) Although the VIPS Memo indicated, correctly, that on June 15, 2016,

“Guccifer 2.0” … posts a document that the forensics show was synthetically tainted with ‘Russian fingerprints,’” other language in the Memo was mistaken in indicating that evidence of such tainting was *also* found in the “Guccifer 2.0” metadata from the copying event on July 5.
