VIPS: Mueller’s Forensics-Free Findings

The final Mueller report should be graded “incomplete,” says VIPS, whose forensic work proves the speciousness of the story that DNC emails published by WikiLeaks came from Russian hacking.

March 13, 2019

MEMORANDUM FOR: The Attorney General

FROM: Veteran Intelligence Professionals for Sanity (VIPS)

SUBJECT: Mueller’s Forensics-Free Findings

Executive Summary

Media reports are predicting that Special Counsel Robert Mueller is about to give you the findings of his probe into any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump. If Mueller gives you his “completed” report anytime soon, it should be graded “incomplete.” Major deficiencies include depending on a DNC-hired cybersecurity company for forensics and failure to consult with those who have done original forensic work, including us and the independent forensic investigators with whom we have examined the data. We stand ready to help.

We veteran intelligence professionals (VIPS) have done enough detailed forensic work to prove the speciousness of the prevailing story that the DNC emails published by WikiLeaks came from Russian hacking. Given the paucity of evidence to support that story, we believe Mueller may choose to finesse this key issue and leave everyone hanging.

That would help sustain the widespread belief that Trump owes his victory to President Vladimir Putin, and strengthen the hand of those who pay little heed to the unpredictable consequences of an increase in tensions with nuclear-armed Russia.

There is an overabundance of “assessments” but a lack of hard evidence to support that prevailing narrative. We believe that there are enough people of integrity in the Department of Justice to prevent the outright manufacture or distortion of “evidence,” particularly if they become aware that experienced scientists have completed independent forensic study that yield very different conclusions. We know only too well – and did our best to expose – how our former colleagues in the intelligence community manufactured fraudulent “evidence” of weapons of mass destruction in Iraq.

We have scrutinized publicly available physical data – the “trail” that every cyber operation leaves behind. And we have had support from highly experienced independent forensic investigators who, like us, have no axes to grind. We can prove that the conventional-wisdom story about Russian-hacking-DNC-emails-for-WikiLeaks is false. Drawing largely on the unique expertise of two VIPS scientists who worked for a combined total of 70 years at the National Security Agency and became Technical Directors there, we have regularly published our findings. But we have been deprived of a hearing in mainstream media – an experience painfully reminiscent of what we had to endure when we exposed the corruption of intelligence before the attack on Iraq 16 years ago.

This time, with the principles of physics and forensic science to rely on, we are able to adduce solid evidence exposing mistakes and distortions in the dominant story. We offer you below – as a kind of *aide-memoire*– a discussion of some of the key factors related to what has become known as "Russia-gate." And we include our most recent findings drawn from forensic work on data associated with WikiLeaks' publication of the DNC emails.

We do not claim our conclusions are "irrefutable and undeniable," a la Colin Powell at the UN before the Iraq war. Our judgments, however, are based on the scientific method – not "assessments." We decided to put this memorandum together in hopes of ensuring that you hear that directly from us.

If the Mueller team remains reluctant to review our work – or even to interview willing witnesses with direct knowledge, like WikiLeaks' Julian Assange and former UK Ambassador Craig Murray, we fear that many of those yearning earnestly for the truth on Russia-gate will come to the corrosive conclusion that the Mueller investigation was a sham.

In sum, we are concerned that, at this point, an incomplete Mueller report will fall far short of the commitment made by then Acting Attorney General Rod Rosenstein "to ensure a full and thorough investigation," when he appointed Mueller in May 2017. Again, we are at your disposal.

Discussion

The centerpiece accusation of Kremlin "interference" in the 2016 presidential election was the charge that Russia hacked

Democratic National Committee emails and gave them to WikiLeaks to embarrass Secretary Hillary Clinton and help Mr. Trump win. The weeks following the election witnessed multiple leak-based media allegations to that effect. These culminated on January 6, 2017 in an evidence-light, rump report misleadingly labeled "Intelligence Community Assessment (ICA)." Prepared by "handpicked analysts" from only three of the 17 U.S. intelligence agencies (CIA, FBI, and NSA), the assessment expressed "high confidence" in the Russia-hacking-to-WikiLeaks story, but lacked so much as a hint that the authors had sought access to independent forensics to support their "assessment."

The media immediately awarded the ICA the status of Holy Writ, choosing to overlook an assortment of banal, full-disclosure-type caveats included in the assessment itself – such as:

> "When Intelligence Community analysts use words such as 'we assess' or 'we judge,' they are conveying an analytic assessment or judgment. …Judgments are not intended to imply that we have proof that shows something to be a fact. … Assessments are based on collected information, which is often incomplete or fragmentary … High confidence in a judgment does not imply that the assessment is a fact or a certainty; such judgments might be wrong."

To their credit, however, the authors of the ICA did make a highly germane point in introductory remarks on "cyber incident attribution." They noted: ***"The nature of cyberspace makes attribution of cyber operations difficult but not impossible. Every kind of cyber operation – malicious or not***

– leaves a trail.” [Emphasis added.]

Forensics

The imperative is to get on that “trail” – and quickly, before red herrings can be swept across it. The best way to establish attribution is to apply the methodology and processes of forensic science. Intrusions into computers leave behind discernible physical data that can be examined scientifically by forensic experts. Risk to “sources and methods” is normally not a problem.

Direct access to the actual computers is the first requirement – the more so when an intrusion is termed “an act of war” and blamed on a nuclear-armed foreign government (the words used by the late Sen. John McCain and other senior officials). In testimony to the House Intelligence Committee in March 2017, former FBI Director James Comey admitted that he did not insist on physical access to the DNC computers even though, as he conceded, “best practices” dictate direct access.

In June 2017, Senate Intelligence Committee Chair Richard Burr asked Comey whether he ever had “access to the actual hardware that was hacked.” Comey answered, “In the case of the DNC … we did not have access to the devices themselves. We got relevant forensic information from a private party, a high-class entity, that had done the work. …” Sen. Burr followed up: “But no content? Isn’t content an important part of the forensics from a counterintelligence standpoint?” Comey: “It is, although what was briefed to me by my folks … is that they had gotten the information from the private party that they needed to understand the

intrusion by the spring of 2016."

The "private party/high-class entity" to which Comey refers is CrowdStrike, a cybersecurity firm of checkered reputation and multiple conflicts of interest, including very close ties to a number of key anti-Russian organizations. Comey indicated that the DNC hired CrowdStrike in the spring of 2016.

Given the stakes involved in the Russia-gate investigation – including a possible impeachment battle and greatly increased tension between Russia and the U.S. – it is difficult to understand why Comey did not move quickly to seize the computer hardware so the FBI could perform an independent examination of what quickly became the major predicate for investigating election interference by Russia. Fortunately, enough data remain on the forensic "trail" to arrive at evidence-anchored conclusions. The work we have done shows the prevailing narrative to be false. We have been suggesting this for over two years. Recent forensic work significantly strengthens that conclusion.

We Do Forensics

Recent forensic examination of the Wikileaks DNC files shows they were created on 23, 25 and 26 May 2016. (On June 12, Julian Assange announced he had them; WikiLeaks published them on July 22.) We recently discovered that the files reveal a FAT (File Allocation Table) system property. ***This shows that the data had been transferred to an external storage device, such as a thumb drive, before WikiLeaks posted them.***

FAT is a simple file system named for its method of

organization, the File Allocation Table. It is used for storage only and is not related to internet transfers like hacking. Were WikiLeaks to have received the DNC files via a hack, the last modified times on the files would be a random mixture of odd-and even-ending numbers.

Why is that important? The evidence lies in the "last modified" time stamps on the Wikileaks files. When a file is stored under the FAT file system the software rounds the time to the nearest even-numbered second. Every single one of the time stamps in the DNC files on WikiLeaks' site ends in an even number.

We have examined 500 DNC email files stored on the Wikileaks site. All 500 files end in an even number—2, 4, 6, 8 or 0. If those files had been hacked over the Internet, there would be an equal probability of the time stamp ending in an odd number. The random probability that FAT was not used is 1 chance in 2 to the 500th power. Thus, these data show that the DNC emails posted by WikiLeaks went through a storage device, like a thumb drive, and were physically moved before Wikileaks posted the emails on the World Wide Web.

This finding alone is enough to raise reasonable doubts, for example, about Mueller's indictment of 12 Russian intelligence officers for hacking the DNC emails given to WikiLeaks. A defense attorney could easily use the forensics to argue that someone copied the DNC files to a storage device like a USB thumb drive and got them physically to WikiLeaks — not electronically via a hack.

Role of NSA

For more than two years, we strongly suspected that the DNC

emails were copied/leaked in that way, not hacked. And we said so. We remain intrigued by the apparent failure of NSA's dragnet, collect-it-all approach – including "cast-iron" coverage of WikiLeaks – to provide forensic evidence (as opposed to "assessments") as to how the DNC emails got to WikiLeaks and who sent them. Well before the telling evidence drawn from the use of FAT, other technical evidence led us to conclude that the DNC emails were not hacked over the network, but rather physically moved over, say, the Atlantic Ocean.

Is it possible that NSA has not yet been asked to produce the collected packets of DNC email data claimed to have been hacked by Russia? Surely, this should be done before Mueller competes his investigation. NSA has taps on all the transoceanic cables leaving the U.S. and would almost certainly have such packets if they exist. (The detailed slides released by Edward Snowden actually show the routes that trace the packets.)

The forensics we examined shed no direct light on who may have been behind the leak. The only thing we know for sure is that the person had to have direct access to the DNC computers or servers in order to copy the emails. The apparent lack of evidence from the most likely source, NSA, regarding a hack may help explain the FBI's curious preference for forensic data from CrowdStrike. No less puzzling is why Comey would choose to call CrowdStrike a "high-class entity."

Comey was one of the intelligence chiefs briefing President Obama on January 5, 2017 on the "Intelligence Community Assessment," which was then briefed to President-elect Trump

and published the following day. That Obama found a key part of the ICA narrative less than persuasive became clear at his last press conference (January 18), when he told the media, “The conclusions of the intelligence community with respect to the Russian hacking were not conclusive … as to how ‘the DNC emails that were leaked’ got to WikiLeaks.

Is Guccifer 2.0 a Fraud?

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the internet as a result of a spearphishing attack. William Binney, one of VIPS’ two former Technical Directors at NSA, along with other former intelligence community experts, examined files posted by Guccifer 2.0 and discovered that those files could not have been downloaded over the internet. It is a simple matter of mathematics and physics.

There was a flurry of activity after Julian Assange announced on June 12, 2016: “We have emails relating to Hillary Clinton which are pending publication.” On June 14, DNC contractor CrowdStrike announced that malware was found on the DNC server and claimed there was evidence it was injected by Russians. On June 15, the Guccifer 2.0 persona emerged on the public stage, affirmed the DNC statement, claimed to be responsible for hacking the DNC, claimed to be a WikiLeaks source, ***and posted a document that forensics show was synthetically tainted with “Russian fingerprints.”***

Our suspicions about the Guccifer 2.0 persona grew when G-2 claimed responsibility for a “hack” of the DNC on July 5, 2016, which released DNC data that was rather bland compared

to what WikiLeaks published 17 days later (showing how the DNC had tipped the primary scales against Sen. Bernie Sanders). As VIPS reportedin a wrap-up Memorandum for the President on July 24, 2017 (titled "Intel Vets Challenge 'Russia Hack' Evidence)," forensic examination of the July 5, 2016 cyber intrusion into the DNC showed it NOT to be a hack by the Russians or by anyone else, but rather a copy onto an external storage device. It seemed a good guess that the July 5 intrusion was a contrivance to preemptively taint anything WikiLeaks might later publish from the DNC, by "showing" it came from a "Russian hack." WikiLeaks published the DNC emails on July 22, three days before the Democratic convention.

As we prepared our July 24 memo for the President, we chose to begin by taking Guccifer 2.0 at face value; i. e., that the documents he posted on July 5, 2016 were obtained via a hack over the Internet. Binney conducted a forensic examination of the metadata contained in the posted documents and compared that metadata with the known capacity of Internet connection speeds at the time in the U.S. This analysis showed a transfer rate as high as 49.1 megabytes per second, which is much faster than was possible from a remote online Internet connection. The 49.1 megabytes speed coincided, though, with the rate that copying onto a thumb drive could accommodate.

Binney, assisted by colleagues with relevant technical expertise, then extended the examination and ran various forensic tests from the U.S. to the Netherlands, Albania, Belgrade and the UK. The fastest Internet rate obtained – from a data center in New Jersey to a data center in the UK

– was 12 megabytes per second, which is less than a fourth of the capacity typical of a copy onto a thumb drive.

The findings from the examination of the Guccifer 2.0 data and the WikiLeaks data does not indicate who copied the information to an external storage device (probably a thumb drive). But our examination does disprove that G.2 hacked into the DNC on July 5, 2016. Forensic evidence for the Guccifer 2.0 data adds to other evidence that the DNC emails were not taken by an internet spearphishing attack. The data breach was local. The emails were copied from the network.

Presidential Interest

After VIPS' July 24, 2017 Memorandum for the President, Binney, one of its principal authors, was invited to share his insights with Mike Pompeo, CIA Director at the time. When Binney arrived in Pompeo's office at CIA Headquarters on October 24, 2017 for an hour-long discussion, the director made no secret of the reason for the invitation: "You are here because the President told me that if I really wanted to know about Russian hacking I needed to talk with you."

Binney warned Pompeo – to stares of incredulity – that his people should stop lying about the Russian hacking. Binney then started to explain the VIPS findings that had caught President Trump's attention. Pompeo asked Binney if he would talk to the FBI and NSA. Binney agreed, but has not been contacted by those agencies. With that, Pompeo had done what the President asked. There was no follow-up.

Confronting James Clapper on Forensics

We, the *hoi polloi,*do not often get a chance to talk to people like Pompeo – and still less to the former intelligence chiefs who are the leading purveyors of the prevailing Russia-gate narrative. An exception came on November 13, when former National Intelligence Director James Clapper came to the Carnegie Endowment in Washington to hawk his memoir. Answering a question during the Q&A about Russian "hacking" and NSA, Clapper said:

"Well, I have talked with NSA a lot … And in my mind, I spent a lot of time in the SIGINT business, ***the forensic evidence was overwhelming about what the Russians had done.*** There's absolutely no doubt in my mind whatsoever." [Emphasis added]

Clapper added: "… as a private citizen, understanding the magnitude of what the Russians did and the number of citizens in our country they reached and the different mechanisms that, by which they reached them, to me it stretches credulity to think they didn't have a profound impact on election on the outcome of the election."

(A transcript of the interesting Q&A can be found hereand a commentary on Clapper's performance at Carnegie, as well as on his longstanding lack of credibility, is here.)

Normally soft-spoken Ron Wyden, Democratic senator from Oregon, lost his patience with Clapper last week when he learned that Clapper is still denying that he lied to the Senate Intelligence Committee about the extent of NSA surveillance of U.S. citizens. In an unusual outburst, Wyden said: "James Clapper needs to stop making excuses for lying to the American people about mass surveillance. To be clear:

I sent him the question in advance. I asked him to correct the record afterward. He chose to let the lie stand."

The materials brought out by Edward Snowden in June 2013 showed Clapper to have lied under oath to the committee on March 12, 2013; he was, nevertheless, allowed to stay on as Director of National Intelligence for three and half more years. Clapper fancies himself an expert on Russia, telling *Meet the Press*on May 28, 2017 that Russia's history shows that Russians are "typically, almost genetically driven to co-opt, penetrate, gain favor, whatever."

Clapper ought to be asked about the "forensics" he said were "overwhelming about what the Russians had done." And that, too, before Mueller completes his investigation.

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 (ret.)

Richard H. Black, Senator of Virginia, 13th District; Colonel US Army (ret.); Former Chief, Criminal Law Division, Office of the Judge Advocate General, the Pentagon (associate VIPS)

Bogdan Dzakovic, former Team Leader of Federal Air Marshals and Red Team, FAA Security (ret.) (associate VIPS)

Philip Giraldi, CIA, Operations Officer (ret.)

Mike Gravel, former Adjutant, top secret control officer, Communications Intelligence Service; special agent of the

Counter Intelligence Corps and former United States Senator

James George Jatras, former U.S. diplomat and former foreign policy adviser to Senate leadership (Associate VIPS)

Larry C. Johnson, former CIA and State Department Counter Terrorism officer

John Kiriakou, former CIA Counterterrorism Officer and former senior investigator, Senate Foreign Relations Committee

Karen Kwiatkowski, former Lt. Col., US Air Force (ret.), at Office of Secretary of Defense watching the manufacture of lies on Iraq, 2001-2003

Edward Loomis, Cryptologic Computer Scientist, former Technical Director at NSA (ret.)

David MacMichael, Ph.D., former senior estimates officer, National Intelligence Council (ret.)

Ray McGovern, former US Army infantry/intelligence officer & CIA analyst; CIA Presidential briefer (ret.)

Elizabeth Murray, former Deputy National Intelligence Officer for the Near East, National Intelligence Council & CIA political analyst (ret.)

Todd E. Pierce, MAJ, US Army Judge Advocate (ret.)

Peter Van Buren, US Department of State, Foreign Service Officer (ret.) (associate VIPS)

Sarah G. Wilton, CDR, USNR, (ret.); Defense Intelligence Agency (ret.)

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

Ann Wright, retired U.S. Army reserve colonel and former U.S. diplomat who resigned in 2003 in opposition to the Iraq War

Veteran Intelligence Professionals for Sanity (VIPS) is made up of former intelligence officers, diplomats, military officers and congressional staffers. The organization, founded in 2002, was among the first critics of Washington's justifications for launching a war against Iraq. VIPS advocates a US foreign and national security policy based on genuine national interests rather than contrived threats promoted for largely political reasons. An archive of VIPS memoranda is available at Consortiumnews.com.