New Cracks in Russia-gate Foundation

The Russia-gate groupthink always rested on a fragile foundation of dubious analysis and biased guesswork, but now has been shaken by new forensic studies of the purported “hack,” as Patrick Lawrence reported at The Nation.

By Patrick Lawrence

It is now a year since the Democratic National Committee’s mail system was compromised — a year since events in the spring and early summer of 2016 were identified as remote hacks and, in short order, attributed to Russians acting in behalf of Donald Trump.

A great edifice has been erected during this time. President Trump, members of his family, and numerous people around him stand accused of various corruptions and extensive collusion with Russians. Half a dozen simultaneous investigations proceed into these matters. Last week news broke that Special Counsel Robert Mueller had convened a grand jury, which issued its first subpoenas on August 3. Allegations of treason are common; prominent political figures and many media cultivate a case for impeachment.

The President’s ability to conduct foreign policy, notably but not only with regard to Russia, is now crippled. Forced into a corner and having no choice, Trump just signed legislation imposing severe new sanctions on Russia and European companies working with it on pipeline projects vital to Russia’s energy sector. Striking this close to the core of another nation’s economy is customarily considered an act of war, we must not forget.

In retaliation, Moscow has announced that the United States must cut its embassy staff by roughly two-thirds. All sides agree that relations between the United States and Russia are now as fragile as they were during some of the Cold War’s worst moments. To suggest that military conflict between two nuclear powers inches ever closer can no longer be dismissed as hyperbole.

All this was set in motion when the DNC’s mail server was first violated in the spring of 2016 and by subsequent assertions that Russians were behind that “hack” and another such operation, also described as a Russian hack, on July 5. These are the foundation stones of the edifice just outlined.

The evolution of public discourse in the year since is worthy of scholarly study: Possibilities became allegations, and these became probabilities. Then the probabilities turned into certainties, and these evolved into what are now taken to be established truths. By my reckoning, it required a few days to a few

weeks to advance from each of these stages to the next. This was accomplished via the indefensibly corrupt manipulations of language repeated incessantly in our leading media.

Lost in a year that often appeared to veer into our peculiarly American kind of hysteria is the absence of any credible evidence of what happened last year and who was responsible for it. It is tiresome to note, but none has been made available. Instead, we are urged to accept the word of institutions and senior officials with long records of deception. These officials profess "high confidence" in their "assessment" as to what happened in the spring and summer of last year — this standing as their authoritative judgment.

Few have noticed since these evasive terms first appeared that an assessment is an opinion, nothing more, and to express high confidence is an upside-down way of admitting the absence of certain knowledge. This is how officials avoid putting their names on the assertions we are so strongly urged to accept — as the record shows many of them have done.

We come now to a moment of great gravity.

There has been a long effort to counter the official narrative we now call "Russiagate." This effort has so far focused on the key events noted above, leaving numerous others still to be addressed. Until recently, researchers undertaking this work faced critical shortcomings, and these are to be explained. But they have achieved significant new momentum in the past several weeks, and what they have done now yields very consequential fruit.

Forensic investigators, intelligence analysts, system designers, program architects, and computer scientists of long experience and strongly credentialed are now producing evidence disproving the official version of key events last year. Their work is intricate and continues at a kinetic pace as we speak. But its certain results so far are two, simply stated, and freighted with implications:

- There was no hack of the Democratic National Committee's system on July 5 last year — not by the Russians, not by anyone else. Hard science now demonstrates it was a leak — a download executed locally with a memory key or a similarly portable data-storage device. In short, it was an inside job by someone with access to the DNC's system. This casts serious doubt on the initial "hack," as alleged, that led to the very consequential publication of a large store of documents on WikiLeaks last summer.
- Forensic investigations of documents made public two weeks prior to the July 5 leak by the person or entity known as Guccifer 2.0 show that they were fraudulent: Before Guccifer posted them they were adulterated by

> cutting and pasting them into a blank template that had Russian as its default language. Guccifer took responsibility on June 15 for an intrusion the DNC reported on June 14 and professed to be a WikiLeaks source — claims essential to the official narrative implicating Russia in what was soon cast as an extensive hacking operation. To put the point simply, forensic science now devastates this narrative.

New Analyses

This article is based on an examination of the documents these forensic experts and intelligence analysts have produced, notably the key papers written over the past several weeks, as well as detailed interviews with many of those conducting investigations and now drawing conclusions from them. Before proceeding into this material, several points bear noting.

One, there are many other allegations implicating Russians in the 2016 political process. The work I will now report upon does not purport to prove or disprove any of them. Who delivered documents to WikiLeaks? Who was responsible for the "phishing" operation penetrating John Podesta's e-mail in March 2016?

We do not know the answers to such questions. It is entirely possible, indeed, that the answers we deserve and must demand could turn out to be multiple: One thing happened in one case, another thing in another. The new work done on the mid-June and July 5 events bears upon all else in only one respect. We are now on notice: Given that we now stand face to face with very considerable cases of duplicity, it is imperative that all official accounts of these many events be subject to rigorously skeptical questioning. Do we even know that John Podesta's e-mail was in fact "phished"? What evidence of this has been produced? Such rock-bottom questions as these must now be posed in all other cases.

Two, houses built on sand and made of cards are bound to collapse, and there can be no surprise that the one resting atop the "hack theory," as we can call the prevailing wisdom on the DNC events, appears to be in the process of doing so.

Neither is there anything far-fetched in a reversal of the truth of this magnitude. American history is replete with similar cases. The Spanish sank the *Maine* in Havana harbor in February 1898. Iran's Mossadegh was a Communist. Guatemala's Árbenz represented a Communist threat to the United States. Vietnam's Ho Chi Minh was a Soviet puppet. The Sandinistas were Communists. The truth of the *Maine*, a war and a revolution in between, took a century to find the light of day, whereupon the official story disintegrated. We can do better now. It is an odd sensation to live through one of these episodes, especially one as big as Russiagate. But its place atop a long line of precedents can no longer be disputed.

Three, regardless of what one may think about the investigations and conclusions I will now outline — and, as noted, these investigations continue — there is a bottom line attaching to them. We can even call it a red line. Under no circumstance can it be acceptable that the relevant authorities — the National Security Agency, the Justice Department (via the Federal Bureau of Investigation), and the Central Intelligence Agency — leave these new findings without reply. Not credibly, in any case. Forensic investigators, prominent among them people with decades' experience at high levels in these very institutions, have put a body of evidence on a table previously left empty. Silence now, should it ensue, cannot be written down as an admission of duplicity, but it will come very close to one.

It requires no elaboration to apply the above point to the corporate media, which have been flaccidly satisfied with official explanations of the DNC matter from the start.

Qualified experts working independently of one another began to examine the DNC case immediately after the July 2016 events. Prominent among these is a group comprising former intelligence officers, almost all of whom previously occupied senior positions. Veteran Intelligence Professionals for Sanity (VIPS), founded in 2003, now has 30 members, including a few associates with backgrounds in national-security fields other than intelligence. The chief researchers active on the DNC case are four: William Binney, formerly the NSA's technical director for world geopolitical and military analysis and designer of many agency programs now in use; Kirk Wiebe, formerly a senior analyst at the NSA's SIGINT Automation Research Center; Edward Loomis, formerly technical director in the NSA's Office of Signal Processing; and Ray McGovern, an intelligence analyst for nearly three decades and formerly chief of the CIA's Soviet Foreign Policy Branch. Most of these men have decades of experience in matters concerning Russian intelligence and the related technologies. This article reflects numerous interviews with all of them conducted in person, via Skype, or by telephone.

The customary VIPS format is an open letter, typically addressed to the President. The group has written three such letters on the DNC incident, all of which were first published by Robert Parry at www.consortiumnews.com. Here is the latest, dated July 24; it blueprints the forensic work this article explores in detail. They have all argued that the hack theory is wrong and that a locally executed leak is the far more likely explanation.

In a letter to Barack Obama dated January 17, three days before he left office, the group explained that the NSA's known programs are fully capable of capturing all electronic transfers of data. "We strongly suggest that you ask NSA for any

evidence it may have indicating that the results of Russian hacking were given to WikiLeaks," the letter said. "If NSA cannot produce such evidence — and quickly — this would probably mean it does not have any."

The day after Parry published this letter, Obama gave his last press conference as President, at which he delivered one of the great gems among the official statements on the DNC e-mail question. "The conclusions of the intelligence community with respect to the Russian hacking," the legacy-minded Obama said, "were not conclusive." There is little to suggest the VIPS letter prompted this remark, but it is typical of the linguistic tap-dancing many officials connected to the case have indulged so as to avoid putting their names on the hack theory and all that derives from it.

Cyber-Evidence

Until recently there was a serious hindrance to the VIPS's work, and I have just suggested it. The group lacked access to positive data. It had no lump of cyber-material to place on its lab table and analyze, because no official agency had provided any.

Donald Rumsfeld famously argued with regard to the WMD question in Iraq, "The absence of evidence is not evidence of absence." In essence, Binney and others at VIPS say this logic turns upside down in the DNC case: Based on the knowledge of former officials such as Binney, the group knew that (1) if there was a hack and (2) if Russia was responsible for it, the NSA would have to have evidence of both. Binney and others surmised that the agency and associated institutions were hiding the absence of evidence behind the claim that they had to maintain secrecy to protect NSA programs.

"Everything that they say must remain classified is already well-known," Binney said in an interview. "They're playing the Wizard of Oz game."

New findings indicate this is perfectly true, but until recently the VIPS experts could produce only "negative evidence," as they put it: The absence of evidence supporting the hack theory demonstrates that it cannot be so. That is all VIPS had. They could allege and assert, but they could not conclude: They were stuck demanding evidence they did not have — if only to prove there was none.

Research into the DNC case took a fateful turn in early July, when forensic investigators who had been working independently began to share findings and form loose collaborations wherein each could build on the work of others. In this a small, new website called www.disobedientmedia.com proved an important catalyst. Two independent researchers selected it, Snowden-like, as the medium

through which to disclose their findings.

One of these is known as Forensicator and the other as Adam Carter. On July 9, Adam Carter sent Elizabeth Vos, a co-founder of Disobedient Media, a paper by the Forensicator that split the DNC case open like a coconut.

By this time Binney and the other technical-side people at VIPS had begun working with a man named Skip Folden. Folden was an IT executive at IBM for 33 years, serving 25 years as the IT program manager in the United States. He has also consulted for Pentagon officials, the FBI, and the Justice Department. Folden is effectively the VIPS group's liaison to Forensicator, Adam Carter, and other investigators, but neither Folden nor anyone else knows the identity of either Forensicator or Adam Carter. This bears brief explanation.

The Forensicator's July 9 document indicates he lives in the Pacific Time Zone, which puts him on the West Coast. His notes describing his investigative procedures support this. But little else is known of him. Adam Carter, in turn, is located in England, but the name is a coy pseudonym: It derives from a character in a BBC espionage series called *Spooks*. It is protocol in this community, Elizabeth Vos told me in a telephone conversation this week, to respect this degree of anonymity.

Kirk Wiebe, the former SIGINT analyst at the NSA, thinks Forensicator could be "someone very good with the FBI," but there is no certainty. Unanimously, however, all the analysts and forensics investigators interviewed for this column say Forensicator's advanced expertise, evident in the work he has done, is unassailable. They hold a similarly high opinion of Adam Carter's work.

Forensicator is working with the documents published by Guccifer 2.0, focusing for now on the July 5 intrusion into the DNC server. The contents of Guccifer's files are known — they were published last September — and are not Forensicator's concern. His work is with the metadata on those files. These data did not come to him via any clandestine means. Forensicator simply has access to them that others did not have. It is this access that prompts Kirk Wiebe and others to suggest that Forensicator may be someone with exceptional talent and training inside an agency such as the FBI.

"Forensicator unlocked and then analyzed what had been the locked files Guccifer supposedly took from the DNC server," Skip Folden explained in an interview. "To do this he would have to have 'access privilege,' meaning a key."

What has Forensicator proven since he turned his key? How? What has work done atop Forensicator's findings proven? How?

The Transfer Rate

Forensicator's first decisive findings, made public in the paper dated July 9, concerned the volume of the supposedly hacked material and what is called the transfer rate – the time a remote hack would require. The metadata established several facts in this regard with granular precision: On the evening of July 5, 2016, 1,976 megabytes of data were downloaded from the DNC's server. The operation took 87 seconds. This yields a transfer rate of 22.7 megabytes per second.

These statistics are matters of record and essential to disproving the hack theory. No Internet service provider, such as a hacker would have had to use in mid-2016, was capable of downloading data at this speed. Compounding this contradiction, Guccifer claimed to have run his hack from Romania, which, for numerous reasons technically called delivery overheads, would slow down the speed of a hack even further from maximum achievable speeds.

What is the maximum achievable speed? Forensicator recently ran a test download of a comparable data volume (and using a server speed not available in 2016) 40 miles from his computer via a server 20 miles away and came up with a speed of 11.8 megabytes per second – half what the DNC operation would need were it a hack. Other investigators have built on this finding. Folden and Edward Loomis say a survey published August 3, 2016, by www.speedtest.net/reports is highly reliable and use it as their thumbnail index. It indicated that the highest average ISP speeds of first-half 2016 were achieved by Xfinity and Cox Communications. These speeds averaged 15.6 megabytes per second and 14.7 megabytes per second, respectively. Peak speeds at higher rates were recorded intermittently but still did not reach the required 22.7 megabytes per second.

"A speed of 22.7 megabytes is simply unobtainable, especially if we are talking about a transoceanic data transfer," Folden said. "Based on the data we now have, what we've been calling a hack is impossible." Last week Forensicator reported on a speed test he conducted more recently. It tightens the case considerably. "Transfer rates of 23 MB/s (Mega Bytes per second) are not just highly unlikely, but effectively impossible to accomplish when communicating over the Internet at any significant distance," he wrote. "Further, local copy speeds are measured, demonstrating that 23 MB/s is a typical transfer rate when using a USB–2 flash device (thumb drive)."

Time stamps in the metadata provide further evidence of what happened on July 5. The stamps recording the download indicate that it occurred in the Eastern Daylight Time Zone at approximately 6:45 pm. This confirms that the person entering the DNC system was working somewhere on the East Coast of the United States.

In theory the operation could have been conducted from Bangor or Miami or

anywhere in between — but not Russia, Romania, or anywhere else outside the EDT zone. Combined with Forensicator's findings on the transfer rate, the time stamps constitute more evidence that the download was conducted locally, since delivery overheads — conversion of data into packets, addressing, sequencing times, error checks, and the like — degrade all data transfers conducted via the Internet, more or less according to the distance involved.

Russian 'Fingerprints'

In addition, there is the adulteration of the documents Guccifer 2.0 posted on June 15, when he made his first appearance. This came to light when researchers penetrated what Folden calls Guccifer's top layer of metadata and analyzed what was in the layers beneath. They found that the first five files Guccifer made public had each been run, via ordinary cut-and-paste, through a single template that effectively immersed them in what could plausibly be cast as Russian fingerprints. They were not: The Russian markings were artificially inserted prior to posting. "It's clear," another forensics investigator self-identified as HET, wrote in a report on this question, "that metadata was deliberately altered and documents were deliberately pasted into a Russianified [W]ord document with Russian language settings and style headings."

To be noted in this connection: The list of the CIA's cyber-tools WikiLeaks began to release in March and labeled Vault 7 includes one called Marble that is capable of obfuscating the origin of documents in false-flag operations and leaving markings that point to whatever the CIA wants to point to. (The tool can also "de-obfuscate" what it has obfuscated.) It is not known whether this tool was deployed in the Guccifer case, but it is there for such a use.

It is not yet clear whether documents now shown to have been leaked locally on July 5 were tainted to suggest Russian hacking in the same way the June 15 Guccifer release was. This is among several outstanding questions awaiting answers, and the forensic scientists active on the DNC case are now investigating it.

In a note Adam Carter sent to Folden and McGovern last week and copied to me, he reconfirmed the corruption of the June 15 documents, while indicating that his initial work on the July 5 documents — of which much more is to be done — had not yet turned up evidence of doctoring.

In the meantime, VIPS has assembled a chronology that imposes a persuasive logic on the complex succession of events just reviewed. It is this:

- On June 12 last year, Julian Assange announced that WikiLeaks had and would publish documents pertinent to Hillary Clinton's presidential campaign.

- On June 14, CrowdStrike, a cyber-security firm hired by the DNC, announced, without providing evidence, that it had found malware on DNC servers and had evidence that Russians were responsible for planting it.
- On June 15, Guccifer 2.0 first appeared, took responsibility for the "hack" reported on June 14 and claimed to be a WikiLeaks source. It then posted the adulterated documents just described.
- On July 5, Guccifer again claimed he had remotely hacked DNC servers, and the operation was instantly described as another intrusion attributable to Russia. Virtually no media questioned this account.

It does not require too much thought to read into this sequence. With his June 12 announcement, Assange effectively put the DNC on notice that it had a little time, probably not much, to act preemptively against the imminent publication of damaging documents. Did the DNC quickly conjure Guccifer from thin air to create a cyber-saboteur whose fingers point to Russia? There is no evidence of this one way or the other, but emphatically it is legitimate to pose the question in the context of the VIPS chronology. WikiLeaks began publishing on July 22. By that time, the case alleging Russian interference in the 2016 elections process was taking firm root. In short order Assange would be written down as a "Russian agent."

By any balanced reckoning, the official case purporting to assign a systematic hacking effort to Russia, the events of mid-June and July 5 last year being the foundation of this case, is shabby to the point taxpayers should ask for their money back. The Intelligence Community Assessment, the supposedly definitive report featuring the "high confidence" dodge, was greeted as farcically flimsy when issued January 6.

Ray McGovern calls it a disgrace to the intelligence profession. It is spotlessly free of evidence, front to back, pertaining to any events in which Russia is implicated.

'Hand-Picked' Analysts

James Clapper, the former director of national intelligence, admitted in May that "hand-picked" analysts from three agencies (not the 17 previously reported) drafted the ICA.

There is a way to understand "hand-picked" that is less obvious than meets the eye: The report was sequestered from rigorous agency-wide reviews. This is the way these people have spoken to us for the past year.

Behind the ICA lie other indefensible realities. The FBI has never examined the DNC's computer servers — an omission that is beyond preposterous. It has instead

relied on the reports produced by Crowdstrike, a firm that drips with conflicting interests well beyond the fact that it is in the DNC's employ. Dmitri Alperovitch, its co-founder and chief technology officer, is on the record as vigorously anti-Russian. He is a senior fellow at the Atlantic Council, which suffers the same prejudice. Problems such as this are many.

"We continue to stand by our report," CrowdStrike said, upon seeing the VIPS blueprint of the investigation. CrowdStrike argues that by July 5 all malware had been removed from the DNC's computers. But the presence or absence of malware by that time is entirely immaterial, because the event of July 5 is proven to have been a leak and not a hack. Given that malware has nothing to do with leaks, CrowdStrike's logic appears to be circular.

In effect, the new forensic evidence considered here lands in a vacuum. We now enter a period when an official reply should be forthcoming. What the forensic people are now producing constitutes evidence, however one may view it, and it is the first scientifically derived evidence we have into any of the events in which Russia has been implicated. The investigators deserve a response, the betrayed professionals who formed VIPS as the WMD scandal unfolded in 2003 deserve it, and so do the rest of us. The cost of duplicity has rarely been so high.

I concluded each of the interviews conducted for this column by asking for a degree of confidence in the new findings. These are careful, exacting people as a matter of professional training and standards, and I got careful, exacting replies.

All those interviewed came in between 90 percent and 100 percent certain that the forensics prove out. I have already quoted Skip Folden's answer: impossible based on the data.

"The laws of physics don't lie," Ray McGovern volunteered at one point.

"It's QED, theorem demonstrated," William Binney said in response to my question. "There's no evidence out there to get me to change my mind." When I asked Edward Loomis, a 90 percent man, about the 10 percent he held out, he replied, "I've looked at the work and it shows there was no Russian hack. But I didn't do the work. That's the 10 percent. I'm a scientist."

Editor's note: In its chronology, VIPS mistakenly gave the wrong date for CrowdStrike's announcement of its claim to have found malware on DNC servers. It said June 15, when it should have said June 14. VIPS has acknowledged the error, and we have made the correction.

Patrick Lawrence is a longtime columnist, essayist, critic, and lecturer, whose

most recent books are *Somebody Else's Century: East and West in a Post-Western World* and *Time No Longer: America After the American Century*. His website is patricklawrence.us. [This article was originally published at The Nation at https://www.thenation.com/article/a-new-report-raises-big-questions-about-last-years-dnc-hack/]
