Veteran Intelligence Professionals for Sanity ask: Was the 'Russian Hack' an inside job?

Editor's introduction: The "Russia-gate" disruption of American policy—from attempts to delegitimise President Donald Trump's election altogether, across to wrecking operations against his intention to improve US-Russian relations—stands or falls with the claim that Russian government agencies meddled in the 2016 Presidential election by hacking into Democratic National Committee (DNC) computers, stealing emails which exposed corruption and duplicity in Hillary Clinton's campaign, and passing them to WikiLeaks. The phrase "Russia hacked the election" has become an article of faith for the American mainstream media and most of the Democratic Party. The document republished below, an open memorandum to Trump issued 24 July by the Veteran Intelligence Professionals for Sanity (VIPS), is the latest blow to that unsubstantiated belief.

VIPS members William Binney and Ray McGovern have insisted since last year that several signs point to a *leak* rather than a *hack* as the source of the DNC material put out via WikiLeaks, DCLeaks, and a cyber persona called "Guccifer 2.0". Binney is retired from the National Security Agency (NSA), where he designed signals intelligence automation, while McGovern was a Central Intelligence Agency (CIA) Russia analyst for decades. When the Office of the Director of National Intelligence released its *Intelligence Community Assessment* on 6 January 2017, "assessing" that Russia had run an "influence campaign" including "cyber operations" against the DNC, VIPS ripped its shoddy analysis and demanded that then-President Barack Obama make public any tangible evidence of "Russian hacking".

Now, independent forensic analysis has revealed why the NSA, with its vast interception capabilities, could not produce such evidence and expressed only "moderate" confidence in several of the Intelligence Community findings: evidence of a hack, with transmission of the stolen data over the internet, does not exist. Rather, the data must have been copied locally from a DNC computer or network to an external device.

We urge you to read and study this new VIPS document carefully. It pulls the rug out from under the "Russian hacking" claim, which has been used to justify the current dangerous escalation of East-West hostility.

Some political aspects of the "Russian hacking" attribution are touched on only slightly in the VIPS memo, such as the "dubious professional record and multiple conflicts of interest" of CrowdStrike, the cybersecurity contractor who told the DNC it had been hacked by Russian government agencies. Also outside the scope of the memo are some other crucial points of context, such as the UK's GCHQ electronic intelligence agency being the first to tip off the Americans that the DNC servers had been hacked by the Russians. These articles from the *AAS* archives help fill out the picture:

AAS, 29 June 2016, Richard Bardon, "'Russian hackers' hysteria: Prelude to a false-flag cyber attack?";

AAS, 11 Jan. 2017, Washington Insider "US Intelligence delivers political construct, not analytical report on 'Russian hacking'" and Richard Bardon, "Obama's 'Russian hacking' lie unravels";

AAS, 18 Jan. 2017, "UK government runs 'Colour Revolution' regime change against Trump", a six-page package on the "dodgy dossier" compiled by "ex"-MI6 man Christopher Steele to tar Trump with the "Russia-gate" brush.

The American spelling and punctuation of the original are retained here, as well as the original subheads. This and earlier VIPS memoranda, including the ones cited in square brackets within the text below, are online at the VIPS web page https://consortiumnews.com/vips-memos/.

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, 2017, data was *leaked (not hacked)* by a person with physical access to DNC computers, and then doctored to incriminate Russia.

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, and that "telltale signs" implicating Russia were then inserted.

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 and doctoring were performed on the East coast of the U.S. Thus far, mainstream media have ignored the findings of these independent studies [Elizabeth Vos, "New Research Shows Guccifer 2.0 Files Were Copied Locally, Not Hacked", disobedientmedia.com, 9 July 2017; "Guccifer 2.0 NGP/VAN Metadata Analysis", The Forensicator website; hyperlinks are given in the text of this release posted on the VIPS page at Consortium News, address shown above].

Independent analyst Skip Folden, a retired 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 [VIPS memoranda "Allegations of Hacking Election are Baseless", 12 Dec. 2016, and "A Demand for Russian 'Hacking' Proof", 17 Jan. 2017].

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 March 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 principles of physics don't lie; and 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 a 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 after being doctored with a cut-and-paste job 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 15, 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: On the same day, "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 & 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 many times 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. Moreover, the forensics performed on the metadata reveal there was a subsequent synthetic insertion—a cut-and-paste job using a Russian template, with the clear aim of attributing the data to a "Russian hack." This was all performed in the East Coast time zone.

"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 "de-obfuscator" 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)

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

US Congress sabotages world security

By Elisa Barwick

A major effort to wreck the only pathway to prevent war and develop a new framework for peace is under way in the US Congress, through a bill that would stop President Donald Trump from keeping his campaign promise to cooperate with Russia. H.R. 3364, the *Countering America's Adversaries Through Sanctions Act of 2017*, was originally an Iran sanctions bill, but was expanded to include North Korea and now Russia, in order to bring to bear false allegations of Russian interference in the 2016 US presidential election. The Senate overwhelmingly voted up the bill (98-2) on 27 July, after the House registered only 3 dissenting votes (with 419 in favour) on 25 July. This puts almost the entire Congress in support of the web of lies known as Russia-gate, within days of a major exposé by Veteran Intelligence Professionals (VIPS) which revealed that there was no hacking of Democratic National Committee (DNC) computers; rather, material which allegedly benefited Trump's campaign was leaked by someone with internal access to DNC servers, for which Russia was framed (p. 10).

Given that the sanctions bill passed with a veto-proof majority, the White House has announced that the President will sign it into law. The legislation includes restrictions to prevent Trump from lifting the sanctions without first seeking Congressional approval. Questions still remain over whether this maneuver to prevent Trump from setting foreign policy, the responsibility of the President and not the Congress, is in breach of the Constitutional separation of powers.

One component of the legislation which has angered European countries as well as Russia, concerns Russian energy exports and development initiatives. The bill expands sanctions levelled by the Obama administration against Russian crude oil projects as well as the Nord Stream 2 gas pipeline, which will bring gas from Russia to Germany, delivering it to central and western Europe across the Baltic sea floor. European companies that cooperate with Russian companies could now be subject to sanctions. German Foreign Minister Sigmar Gabriel has said the sanctions are unacceptable and that Europe will respond appropriately.

Further, the "Countering the Russian influence in Europe and Eurasia" section of the bill states that Russia "has sought to exert influence throughout Europe and Eurasia, including in the former states of the Soviet Union". This takes aim at Russia's collaborative efforts with China to bring more nations into the Greater Eurasia project, formed by the intersection of development initiatives launched by the Belt and Road Initiative (BRI), Eurasian Economic Union (EAEU), and Shanghai Cooperation Organisation (SCO).

Reacting to the bill during a visit to Finland, Russian President Vladimir Putin declared that amid constant provocations Russia is responding with patience, although he hinted that a more serious response could follow at a certain point. Putin still insisted that the United States and Russia must achieve at least a minimum level of cooperation and agreement. He situated the entire affair as driven by American "domestic political disputes", saying it was "deeply regrettable" that Russian-US relations had fallen victim to them.

On 28 July Russia finally retaliated for the seizure of its diplomatic facilities and expulsion of diplomats in December 2016, ordered by former President Barack Obama Administration to punish unproven Russian election meddling through "significant malicious cyber-enabled activities" (hacking). US diplomatic staff in Russia will be brought down to the level of Russian staff in the USA, a reduction by 755 individuals, and two US facilities in Moscow must be surrendered. Russian Foreign Minister Sergei Lavrov told US Secretary of State Rex Tillerson by phone that he hoped the Russian actions cause Washington to reflect on its policies. "US politics have been captured by the Russophobic forces that have been pushing Washington towards the path of confrontation", reported a Russian Foreign Ministry statement, but Lavrov affirmed that Russia remains ready to normalise relations on the basis of equality, mutual respect and a balance of interests.

During 17-18 July talks, Russian Deputy Foreign Minister Sergei Ryabkov and US Under Secretary of State for Political Affairs Thomas Shannon initiated a "strategic stability dialogue" between the USA and Russia, as agreed between Lavrov and Tillerson in April and confirmed when Putin and Trump met in Germany on 7 July. Ryabkov said there would be a continuing "bilateral interagency exchange on a number of issues related to maintaining strategic stability between Russia and the United States".

A better potential

Following the Trump-Putin meeting on the sidelines of the G20 Hamburg Summit, and Trump's subsequent visit to French President Emmanuel Macron in Paris, it is possible to envision a shift in the global strategic geometry, with the beginnings of collaboration to de-escalate hotspots such as Syria and North Korea. These efforts are visible in the growing regions of ceasefire in Syria, and end of American and French insistence on the removal of Syrian President Bashar al-Assad as prerequisite for peace. France has tempered its position on cooperation with Russia, and German Foreign Minister Gabriel called for détente with Russia in *Focus* magazine on 16 July.

China and Russia are establishing a framework the USA can slot into regarding North Korea. Discussions between Putin and Chinese President Xi Jinping in Moscow before the G20 meeting continued among high-level officials at the 7th Russian-Chinese Dialogue on Security in Northeast Asia, held in Beijing on 20 July. While mutual concern about North Korea's ongoing missile tests was expressed, an agreement to promote positive shifts in the situation was reached. Russia sent an envoy to North Korea for six days on 23 July, as part of the Russian-Chinese effort to set up new talks. The US Navy and the Chinese People's Liberation Army Navy held a video conference on 20 July, with US Chief of Naval Operations Admiral John Richardson asking PLA Navy Commander Vice Admiral Shen Jinlong for support in monitoring North Korean missile launches, including possible ones from submarines.

The potential for three-way collaboration between the USA, China and Russia has enormous implications for stabilising the world. But first, the "time bombs" left by the Obama Administration and perpetuated by the Congress, which threaten to blow up the relations Trump has established with Putin and Xi, must be defused.