ELECTION 2016 US INTELLIGENCE DEMOCRATIC NATIONAL COMMITTEE

A Leak or a Hack? A Forum on the VIPS Memo

A letter from dissenting members of VIPS, a reply from VIPS, and the results of our independent review.

By Various Contributors

SEPTEMBER 1, 2017

The Democratic National Committee headquarters, October 27, 2016. *(Sipa via AP Images)*

Editor's note, 9/1/2017: For more than 150 years, *The Nation* has been committed to fearless, independent journalism. We have a long history of seeking alternative views and taking unpopular stances. We believe it is important to challenge questionable conventional wisdom and to foster debate—not police it. Focusing on unreported or inadequately reported issues of major importance and raising questions that are not being asked have always been a central part of our work.

This journalistic mission led *The Nation* to be troubled by the paucity of serious public scrutiny of the January 2017 intelligence-community assessment (ICA) on purported Russian interference in our 2016 presidential election, which reflects the judgment of the CIA, the FBI, and the NSA. That report concluded that Russian President Vladimir Putin personally ordered the hacking of the DNC and the dissemination of e-mails from key staffers via WikiLeaks, in order to damage Hillary Clinton's candidacy. This official intelligence assessment has since led to what some call "Russiagate," with charges and investigations of alleged collusion with the Kremlin, and, in turn, to what is now a major American domestic political crisis and an increasingly perilous state of US-Russia relations. To this day, however, the intelligence agencies that released this assessment have failed to provide the American people with any actual evidence substantiating their claims about how the DNC material was obtained or by whom. Astonishingly and often overlooked, the authors of the declassified ICA themselves admit that their "judgments are not intended to imply that we have proof that shows something to be a fact."

That is why *The Nation* published Patrick Lawrence's article "A New Report Raises Big Questions About Last Year's DNC Hack." The article largely reported on a recently published memo prepared by Veteran Intelligence Professionals for Sanity (VIPS), which argued, based on their own investigation, that the theft of the DNC e-mails was not a hack, but some kind of inside leak that did not involve Russia.

VIPS, formed in 2003 by a group of former US intelligence officers with decades of experience working within the CIA, the FBI, the NSA, and other agencies, previously produced some of the most credible—and critical—analyses of the Bush administration's mishandling of intelligence data in the run-up to the 2003 invasion of Iraq.

The most recent VIPS memo, released on July 24, whatever its technical merits, contributes to a much-needed critical discussion. Despite all the media coverage taking the veracity of the ICA assessment for granted, even now we have only the uncorroborated assertion of intelligence officials to go on. Indeed, this was noticed by *The New York Times*'s Scott Shane, who wrote the day the report appeared: "What is missing from the public report is...hard evidence to back up the agencies' claims that the

Russian government engineered the election attack.... Instead, the message from the agencies essentially amounts to 'trust us.'"

As editor of *The Nation*, my purpose in publishing Patrick Lawrence's article was to make more widely known the VIPS critique of the January ICA assertions, the questions VIPS raised, and their counter-thesis that the disseminated DNC e-mails resulted from a leak, not a hack. Those questions remain vital.

Subsequently, *Nation* editors themselves raised questions about the editorial process that preceded the publication of the article. The article was indeed fact-checked to ensure that Patrick Lawrence, a regular *Nation* contributor, accurately reported the VIPS analysis and conclusions, which he did. As part of the editing process, however, we should have made certain that several of the article's conclusions were presented as possibilities, not as certainties. And given the technical complexity of the material, we would have benefited from bringing on an independent expert to conduct a rigorous review of the VIPS technical claims.

We have obtained such a review in the last week from Nathan Freitas of the Guardian Project. He has evaluated both the VIPS memo and Lawrence's article. Freitas lays out several scenarios in which the DNC could have been hacked from the outside, although he does not rule out a leak. Freitas concludes that all parties "must exercise much greater care in separating out statements backed by available digital metadata from thoughtful insights and educated guesses." His full findings are published below.

We have also learned since publication, from longtime VIPS member Thomas Drake, that there is a dispute among VIPS members themselves about the July 24 memo. This is not the first time a VIPS report has been internally disputed, but it is the first time one has been released over the substantive objections of several VIPS members. With that in mind, we asked Drake and those VIPS members who agree with him to present their dissenting view. We also asked VIPS members who stand by their report to respond. Their comments are also below.

In presenting this follow-up, *The Nation* hopes to encourage further inquiry into the crucial questions of how, why, and by whom the DNC e-mails were made public—a matter that continues to roil our politics. We especially hope that other people with special expertise or knowledge will come forward.

—Katrina vanden Heuvel, editor and publisher

.

WHEN FACTS ARE NOT FACTS

BY THOMAS DRAKE, SCOTT RITTER, LISA LING, CIAN WESTMORELAND, PHILIP M. GIRALDI, AND JESSELYN RADACK

The recent article published on August 9, 2017, in *The Nation* by Patrick Lawrence leans heavily on a July 24, 2017, Veteran Intelligence Professionals for Sanity (VIPS) memo published by *Consortiumnews.com* and then picked up by several media outlets.

However, a number of VIPS members did not sign this problematic memo because of troubling questions about its conclusions, and others who did sign it have raised key concerns since its publication.

The heart of the VIPS memo centers on two statements that relate to an alleged "Guccifer 2.0" cyber-attack against the Democratic National Committee (DNC):

- "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."

Two critical analytic issues emerge from these statements. First, the intelligence-community assessment from January 6, 2017, which reflects the judgment of the CIA, the FBI, and the NSA, asserts as fact (absent categorical proof or evidence) that "Guccifer 2.0" accessed data from the DNC through a "cyber operation." This could mean via the network, the cloud, computers, remote hacking, or direct data removal. However, "Guccifer 2.0" claimed access to the DNC server through remote hacking.

The third-party analysis of the "Guccifer 2.0" claims (including from Adam Carter and the Forensicator) analyzed in the VIPS memo directly contradict these conclusions (while raising legitimate questions), but the VIPS memo asserts as a "slam dunk" fact the categorical conclusion of a local leak that is not supported by the third-party analysis either. There is also no evidence from the available metadata that can definitively state when the transfer or copying of the data took place, nor does the data prove that "Guccifer 2.0" had direct access to the DNC server or that the data was located on the DNC system when it was allegedly copied on July 5, 2016.

The implications of this leap-to-conclusions analysis of the VIPS memo—which centers on claiming as an unassailable and immutable fact that the DNC "hack" was committed by an insider with direct access to the DNC server, who then deliberately doctored data and documents to look like a Russian or Russia-affiliated actor was involved, and therefore no hack occurred (consequently, ipso facto, the Russians did not do it) —are contingent on a fallacy.

Data-transfer speeds across networks and the Internet measured in megabits per second (or megabytes per second) can easily achieve rates that greatly exceed the cited reference in the VIPS memo of 1,976 megabytes in 87 seconds (~22.71 megabytes per second or ~181.7 megabits per second), and well beyond 50 megabytes, depending on the capacity of the network and the method of access to that network. Speeds across the network vary greatly, and sustained write speeds copied out to local devices are often quite a bit slower.

The environment around Trump, Russia, et al. is hyperpolarized right now, and much disinformation is floating around, feeding confirmation bias, mirroring and even producing conspiracy theories.

However, this VIPS memo could have easily raised the necessary and critical questions without resorting to law-of-physics conclusions that claim to prove beyond any shadow of a doubt that it was an inside-network copy only and then asserting the "fact" that the Russians (or anybody else for that matter) did not hack the DNC.

In addition, no qualifiers, disclaimers, or dissenting views are provided in the VIPS memo, nor is any alternative theory presented.

It is important to note that it's equally plausible that the cited July 5, 2016, event was carried out on a server separate from the DNC or elsewhere, and with data previously copied, transferred, or even exfiltrated from the DNC.

However, independent of transfer/copy speeds, if the data was not on the DNC server on July 5, 2016, then none of this VIPS analysis matters (including the categorically stated fact that the local copy was acquired by an insider) and simply undermines the credibility of any and all analysis in the VIPS memo when joined with this flawed predicate.

In addition, a subsequent post by the "Forensicator" actually backs away from the VIPS memo and provides additional caveats, including the following statements:

- "The Guccifer 2.0 NGP/VAN Metadata Analysis describes a copy operation that (based on the metadata) occurred in the early evening on July 5, 2016. No claim is made in the report that the data might not have been copied earlier nor whether it might have been copied or leaked."

- “No claim was made in the Forensicator’s analysis that this computer was connected to a DNC server.”

- “There may be other over-ambitious extrapolations made by the VIPS in their report.”

Furthermore, a recent article in the *New York Post* raises the specter of yet other alternative paths for one or more DNC data breaches. Scott Ritter, a VIPS member, also wrote an article in *Truthdig* that takes issue with the centerpiece claims of the VIPS memo.

The bottom line: This VIPS memo was hastily written based on a flawed analysis of third-party analyses and then thrown against the wall, waiting to see if it would stick. This memo could have cited the critical questions raised in the third-party analyses of “Guccifer 2.0” while also asking why the three US intelligence agencies have yet to provide any actual hard proof following their January 6, 2017, assessment.

The VIPS memo is now increasingly politicized because the analysis itself was politicized. It deals only with alleged “Guccifer 2.0” hacking and makes the classic apples-versus-oranges mistake. In an ideal world, VIPS would at least retract its assertion of certainty. Absent real facts regarding proof of leaks or hacks (or both), how many hypotheses can one copy onto the head of a digital pin?

Signed,

Thomas Drake is a former senior executive at the National Security Agency. Previously, he worked in industry as a principal and consultant in information management and technology, was a naval intelligence officer, served at the CIA as an analyst, and in the Air Force as a crypto-linguist and signals intelligence aircrew member.

Scott Ritter spent 10 years as a Marine Corps intelligence officer, with service in the former Soviet Union and under Gen. H. Norman Schwarzkopf during the first Gulf War. From 1991 to 1998, he served as a chief weapons inspector with the United Nations in Iraq. Today, he consults on energy-intelligence issues.

Lisa Ling (@ARetVet) served in the US military as a technical sergeant on drone surveillance systems before leaving with an honorable discharge in 2012. She appears in the 2016 documentary on drone warfare, *National Bird.*

Cian Westmoreland is an unmanned aircraft systems (UAS) whistle-blower. He is a former transmissions-systems technician who served in a unit establishing battlefield command, control, communication, computing, and intelligence (C4I) capabilities for

Reapers, Predators, and other networked aircraft over the 253,000 square miles of Afghanistan in 2009, in the 73rd Expeditionary Air Control Squadron, before speaking out about the drone program.

Philip M. Giraldi is a former counterterrorism specialist who served for 19 years with the CIA and Army intelligence in Europe and the Middle East. He is executive director of the Council for the National Interest, a Washington-based advocacy group that promotes a foreign policy based on actual US interests. In 2008 and 2012, he was a foreign-policy adviser for presidential candidate Ron Paul. Giraldi is a contributing editor for *The American Conservative* and *The Unz Review*, where he writes about terrorism, intelligence, and national-security issues.

Jesselyn Radack is director of the Whistleblower and Source Protection Program (WHISPeR) at ExposeFacts. Previously, she was a legal adviser with the Justice Department.

* * *

WHY THIS IS IMPORTANT

BY WILLIAM BINNEY, SKIP FOLDEN, ED LOOMIS, RAY MCGOVERN, AND KIRK WIEBE

We Veteran Intelligence Professionals for Sanity (VIPS) scientists make our technical judgments based on given facts and do not speculate without a factual basis. The main issue here is: Who gave the DNC e-mails to WikiLeaks? “Handpicked” analysts from three intelligence agencies “assess” that the Russians hacked into the DNC, but provide no hard evidence for this.

We think back to the evidence-free “assessments” 15 years ago before the attack on Iraq. Several “high-confidence” intelligence judgments had been fraudulently “fixed” to dovetail with the Bush/Cheney agenda for war. In June 2008, the chair of the Senate Intelligence Committee released a bipartisan report five years in the making. Mincing no words, he wrote: “In making the case for war, the Administration repeatedly presented intelligence as fact when in reality it was unsubstantiated, contradicted, or even non-existent.”

We worry that this may be happening again. Adding to our concern, in recent years we have seen “false-flag” attacks carried out to undergird a political narrative and objective—to blame the Syrian government for chemical attacks, for example. Forensic evidence suggests that this tried-and-tested technique (in this instance, simply pasting in a Russian template with “telltale signs”) may have been used to “show” that Russia hacked into the DNC computers last June.

For more than a year, we have been pointing out that any data acquired by a hack would have had to come across the Internet. The blanket coverage of the Internet by the NSA, its UK counterpart GCHQ, and others would be able to produce copies of that data and show where the data originated and where it went. But US intelligence has produced no evidence that hacking by Russia led to it acquiring the DNC e-mails and passing them on to WikiLeaks.

Historically, the United States has disclosed classified information when it has suited its purposes. One need not go all the way back to the release of U-2 photography during the Cuban missile crisis, or to President Ronald Reagan's decision to sacrifice a lucrative source (which enabled us to intercept and decipher Libyan communications) to prove that Libya was behind the April 5, 1986, bombing of a Berlin disco that killed two and wounded 79 US servicemen. Much more recently, in 2014 and 2015, the United States released significant details to verify the successful hack by which China stole over 21.5 million official records, including security background investigations, from the Office of Personnel Management.

Independent research into the metadata associated with the July 5, 2016, cyber-event that was blamed on "Russian hacking" shows that what actually took place was a copy onto an external storage device, and that the copy took place on the East Coast of the United States by someone with physical access to the DNC server or computers. Most curiously, the FBI did not have access to the DNC computers to do its own forensics, even though prominent politicians were calling the alleged Russian hack "an act of war."

After examining the recent forensic findings, Skip Folden, co-author of the VIPS memo titled "Was the 'Russian Hack' an Inside Job?," sent a more detailed technical report to the offices of Special Counsel Robert Mueller and of Attorney General Jeff Sessions, asking them to investigate the latest findings.

We will not dwell on the nontechnical evidence at hand, but we would be remiss if we did not mention something that has recently been in the public eye. Julian Assange has denied that the source is the Russian government or any other state party, and, truth be told, his record of credibility compares favorably with the records of those who demonize him. An associate of Assange, former UK ambassador Craig Murray, has said the WikiLeaks source was a leak from an insider. "To my certain knowledge," said Murray, "neither the DNC nor the Podesta leaks involved Russia." Oddly, Murray has not been questioned by any US official or journalist.

Commentary on the Dissenting Memo

What follows are our comments on the dissenting memo written by Thomas Drake, Lisa Ling, Cian Westmoreland, Philip M. Giraldi, and Jesselyn Radack.

In the words of the memo:

> *[T]he intelligence-community assessment from January 6, 2017, which reflects the judgment of the CIA, the FBI, and the NSA, asserts as fact (absent categorical proof or evidence) that "Guccifer 2.0" accessed data from the DNC through a "cyber operation." This could mean via the network, the cloud, computers, remote hacking, or direct data removal. However, "Guccifer 2.0" claimed access to the DNC server through remote hacking.*

With this statement at the outset, the dissent injects uncertainty about what the words "cyber operation" might include in a way that clearly implies that the Russians could have gotten the DNC e-mails in some way other than through an Internet hack—a very key point. Yes, the January 6 report does use the phrase "cyber operation," but President Obama's intelligence chiefs, including former FBI director James Comey, have testified under oath that they accept CrowdStrike's analysis regarding a "hack." Moreover, intelligence officials have briefed *The New York Times*, *The Washington Post*, and other major news outlets about the alleged Russian role in a hack. In this light, focusing on the phrase "cyber operation" amounts to a word game.

Moreover, does the dissent have proof that the "Guccifer 2.0" "claim" is not fake news? Is the writer of the post at "Guccifer 2.0" actually the person(s) responsible for the data heist? The intelligence-community assessment was not backed up with facts; we cannot believe what it says until technical evidence is provided to prove it.

In the words of the memo:

> *The third-party analysis of the "Guccifer 2.0" claims (including Adam Carter's (g-2.space) and the Forensicator's (theforensicator.wordpress.com/guccifer-2-ngp-van-metadata-analysis)) analyzed in the VIPS memo directly contradict these conclusions (while raising legitimate questions), but the VIPS memo asserts as a "slam dunk" fact the categorical conclusion of a local leak that is also not supported by the third-party analysis, either.*

If we understand this sentence correctly, and the "third-party" analysis refers to the Forensicator, this assertion is wrong. From the data given, the analysis does support the conclusion, as it demonstrates that the Internet on July 5, 2016, could not support such an international hack.

In the words of the memo:

> *There is also no evidence from the available metadata that can definitively state when the transfer or copying of the data took place, nor does the data prove that "Guccifer 2.0" had direct access to the DNC server or that the data was located on the DNC system when it was allegedly copied on July 5, 2016.*

We have no evidence that the July 5 data was manipulated. Nor does the dissent present any. Furthermore, "Guccifer 2.0" bracketed it with his July 4 and 6 posts, which are repeatedly ignored by the dissent. The independent analysis makes no claim that "Guccifer 2.0" had direct access to the DNC server or that the data was located on the server at that time. The transfer rate was independent of the physical location of the data at the time of copy.

In the words of the memo:

> *The implications of this leap-to-conclusions analysis of the VIPS memo—which centers on claiming as an unassailable and immutable fact that the DNC "hack" was committed by an insider with direct access to the DNC server, who then deliberately doctored data and documents to look like a Russian or Russia-affiliated actor was involved, and therefore no hack occurred (consequently, ipso facto, the Russians did not do it)—are contingent on a fallacy.*

There had to be direct access to the DNC server at some point, for that repository was the source of the data. The authors of the dissent are confusing the July 5 and June 15 incidents, for it was the latter that experienced the deliberate insertion of Russian "fingerprints."

In the words of the memo:

> *Data-transfer speeds across networks and the Internet measured in megabits per second (or megabytes per second) can easily achieve rates that greatly exceed the cited reference in the VIPS memo of 1,976 megabytes in 87 seconds (~22.71 megabytes per second or ~181.7 megabits per second), and well beyond 50 megabytes depending on the capacity of the network and the method of access to that network. Speeds across the network vary greatly, and sustained write speeds copied out to local devices are often quite a bit slower.*

The dissent misses the key point of the difference between available speeds in early July 2016 and now. In addition, the above shows no awareness of the degradation of speed with distance and no awareness of the problem of transoceanic connections.

In the words of the memo:

> *The environment around Trump, Russia, et al. is hyperpolarized right now, and much disinformation is floating around, feeding confirmation bias, mirroring and*

> *even producing conspiracy theories.*
>
> *However, this VIPS memo could have easily raised the necessary and critical questions without resorting to law-of-physics conclusions that claim to prove beyond any shadow of a doubt that it was an inside-network copy only and then asserting the "fact" that the Russians (or anybody else for that matter) did not hack the DNC.*

The authors of the dissent may not like the conclusions, but that is exactly what the independent analysis demonstrated, not just via metadata but also by actual network field tests.

In the words of the memo:

> *In addition, no qualifiers, disclaimers, or dissenting views are provided in the VIPS memo, nor is any alternative theory presented.*

The conclusions of our VIPS memo were definitive and included extensive support data if one looks at the websites that were referred to. The writers of the dissent made no attempt to weigh in on the article with a dissenting view or an alternate theory prior to publication of the VIPS memo. Like everyone else, they had two weeks.

In the words of the memo:

> *It is important to note that it's equally plausible that the*

> *cited July 5, 2016, event was carried out on a server separate from the DNC or elsewhere, and with data previously copied, transferred, or even exfiltrated from the DNC.*

Yes, the claimed "hack" could have been done on a secondary computer (not "server"), but in either case had to come originally from the DNC server. This has no effect on the transfer rate, which precluded a "hack"—a point the authors of the dissenting memo keep missing.

In the words of the memo:

> *However, independent of transfer/copy speeds, if the data was not on the DNC server on July 5, 2016, then none of this VIPS analysis matters (including the categorically stated fact that the local copy was acquired by an insider) and simply undermines the credibility of any and all analysis in the VIPS memo when joined with this flawed predicate.*

The dissent refers to "independent of transfer/copy speeds," but one cannot simply ignore them, as if they were irrelevant. Also, again, the "Guccifer 2.0" July 4 and 6 posts are being ignored. The dissent's argument ignores the fact that on July 5, the data was transferred at a speed not obtainable from East Coast ISPs. The transfer rate, however, is entirely consistent with a USB port connected to a portable device such as a thumb drive.

As the author of *The Nation* article pointed out, our investigations continue. Recent data analysis gives additional support to our key finding—namely, that the speed of the data transfer from the DNC server (22.7 megabytes per second) far exceeded the capability of the Internet in early July 2016. We have now learned that the 22.7-megabytes-per-second speed was merely the *average* rate for the duration of the data transfer, and that a peak rate of 38 megabytes per second was reached during that transfer. A copy to a thumb drive could handle that peak speed; an Internet hack attempted from abroad could not.

In the words of the memo:

> *In addition, a subsequent post by the "Forensicator" actually backs away from the VIPS memo and provides additional caveats, including the following statements (among several):*
>
> *"The Guccifer 2.0 NGP/VAN Metadata Analysis describes a copy operation that (based on the metadata) occurred in the early evening on July 5, 2016. No claim is made in the report that the data might not have been copied earlier nor whether it might have been copied or leaked."*

This is correct, but has no bearing on the conclusions.

Direct access was required in either case, whether the alleged "hack" occurred on the DNC server or on a copy made earlier by a person with direct access. The Forensicator is trying, with these later details, to assist those who were confused.

In the words of the memo:

> *Furthermore, a recent article in the* New York Post *raises the specter of yet other alternative paths for one or more DNC data breaches. Scott Ritter, a VIPS member, also wrote an article in* Truthdig *that takes issue with the centerpiece claims of the VIPS memo.*

He did, and without mentioning it to VIPS colleagues more technically experienced in these issues. And the *Truthdig* article contained misstatements of fact, as detailed in e-mails sent within VIPS, including to Ritter, on July 31 regarding claims that the VIPS conclusions are not supported by data, that the transfer rate is irrelevant, etc. It is not clear why the authors of the dissent think that referring to that article poses any challenge to the technical basis for the conclusion that the July 5 metadata was extracted onto a thumb drive. Again, no facts are presented to infer another path.

In the words of the memo:

> *The bottom line: This VIPS memo was hastily written based on a flawed analysis of third-party analyses and*

> *then thrown against the wall, waiting to see if it would stick. This memo could have cited the critical questions raised in the third-party analyses of "Guccifer 2.0" while also asking why the three US intelligence agencies have yet to provide any actual hard proof following their January 6, 2017, assessment.*

Flawed analysis? The dissent has presented no evidence of that. Many of the points raised suggest the authors do not fully understand the analysis. With respect to the alleged hacking and the intelligence-community assessment, the VIPS memo pointed to the parallel report to both the Office of Special Counsel and the attorney general, which covers those issues.

In the words of the memo:

> *The VIPS memo is now increasingly politicized because the analysis itself was politicized. In an ideal world, VIPS would at least retract its assertion of certainty. It only deals with alleged "Guccifer 2.0" hacking and makes the classic apples-versus-oranges mistake. In an ideal world, VIPS would at least retract its assertion of certainty. Absent real facts regarding proof of leaks or hacks (or both), how many hypotheses can one copy onto the head of a digital pin?*

This paragraph is not only misleading, it also impugns the core apolitical nature of VIPS. Again, the dissent seems confused about the main subjects of this discussion and the VIPS memo's key conclusion—that the July 5, 2016, intrusion into the DNC e-mails, which was blamed on Russia, could not have been a hack—by Russia or anyone else. In that very important forest it is difficult to see through all the bushes and trees on which the dissent chooses to focus.

Signed,

William Binney was a civilian employee of the National Security Agency from 1970 to 2001. He held numerous positions, including technical director of the World Geopolitical and Military Analysis Reporting Group; Operations Directorate analysis skill field leader; member of the NSA Senior Technical Review Panel; chair of the Technical Advisory Panel to the Foreign Relations Council; co-founder of the SIGINT Automation Research Center; NSA representative to the National Technology Alliance Executive Board; and technical director of the Office of Russia, as well as working as a senior analyst for Warning for over 20 years. After retiring, Binney blew the whistle on the unconstitutional surveillance programs run by the NSA. His outspoken criticism led to an early-morning FBI raid on his home in 2007. Even before Edward Snowden's whistle-blowing, Binney publicly revealed that the

NSA had access to telecommunications companies' domestic and international billing records, and that since 9/11 the agency has intercepted some 15 to 20 trillion domestic communications. The documents released by Edward Snowden confirmed many of the surveillance dangers about which Binney had been warning under both the Bush and Obama administrations.

Skip Folden (Associate VIPS) retired from IBM after 25 years. His last position there was as IBM program manager for information technology, US.

Ed Loomis is a former NSA technical director for the Office of Signals Processing. From 1996 to 2001, he led the SIGINT Automation Research Center. He retired in 2001 as senior cryptologic computer scientist after 37 years at the agency. He worked for the NSA as an enterprise senior system architect from 2002 to 2007 following retirement, and he was professionally certified in multiple fields at the NSA: mathematician, computer systems analyst, operations research analyst, and system acquisition manager. Loomis applied technical knowledge and experience in developing automated systems focused on producing intelligence supporting military operations and top US decision-makers from 1964 to 2001.

Ray McGovern worked as a CIA analyst under seven presidents and nine CIA directors after serving as a US Army infantry/intelligence officer in the 1960s, McGovern. His concentration was on Russia, one of the foreign posts in which he served. He was chief of the CIA's Foreign Policy Branch in the 1970s and acting national intelligence officer for Western Europe in the '80s. He prepared the President's Daily Brief for Presidents Nixon, Ford, and Reagan. During Reagan's first term, McGovern conducted the early-morning CIA substantive briefings, one-on-one, to the president's five most senior foreign-policy advisers. At retirement, he was awarded the Intelligence Commendation Medallion for "especially meritorious service," but gave it back in March 2006 to dissociate himself from an agency engaged in torture. After retirement, he co-founded Veteran Intelligence Professionals for Sanity.

Kirk Wiebe is a former senior analyst at the SIGINT Automation Research Center, NSA. He led the center's response to National Security Decision Directive 178, ordering the NSA to develop a program to counter the threat posed by foreign relocatable targets, which earned him the DCI's National Meritorious Unit Citation. Wiebe was awarded the NSA's second-highest honor, the Meritorious Civilian Service Award, together with numerous other awards for work on the challenges of digital-age strategic planning. He held the NSA's professional certification as a Russian linguist.

Live links to VIPS memos can be found at consortiumnews.com/vips-memos.

* * *

INDEPENDENT REVIEW OF REPORTING AND ANALYSIS ON THE 2016 COMPROMISE OF THE DNC COMPUTER NETWORK

NATHANIAL FREITAS
FOUNDER, GUARDIAN PROJECT
TECHNICAL DIRECTOR, TIBET ACTION INSTITUTE
AFFILIATE FELLOW, BERKMAN KLEIN CENTER AT HARVARD UNIVERSITY
KEYBASE.IO/N8FR8
PGP: 0X69B37AA9

Background: This document provides an independent technical review of statements made in Patrick Lawrence's article "A New Report Raises Big Questions About Last Year's DNC Hack" that appeared on *The Nation* on August 9, 2017. Claims made in the article were built upon a digital forensic analysis published by a pseudonymous researcher named "the Forensicator" and a memo published by the Veteran Intelligence Professionals for Sanity (VIPS). In addition, related to documents provided by "Guccifer 2.0," there was also a review of information provided by Adam Carter. The focus of the Forensicator's analysis was on the NGP/VAN file archive, distributed by WikiLeaks, in relation to security compromises of computing resources managed by the Democratic National Committee (DNC) in 2016.

This independent review was done at the request of *The Nation* and was undertaken without compensation of any kind.

Relevant Experience: I have developed security and privacy-focused software for enterprise and mobile communications platforms and services for nearly 20 years. I have also acted as a technical resource for a variety of targeted nonprofit activist organizations and communities for 15 years. These groups have faced some of the most sophisticated adversaries in the world, who have, on many occasions, successfully executed attacks against them. Through malicious software, remote-access trojans, and e-mail-link phishing attacks, the private data and communications of these communities have been compromised. The most well-known of these incidents are GhostNet, the targeted attacks on Google originating from China, and the use of Android malware against Tibetan activists.

Summary Findings: The work of the Forensicator is detailed and accurate. There are no significant errors in the specific findings, relating to the analysis of time stamps and calculations related to digital-transfer speeds (also known as "throughput") between storage drives or over a network connection. The Forensicator has worked carefully with the limited set of data available, providing the means necessary for anyone to reproduce the work and analysis.

It is very important to note the set of evidence considered within the Forensicator's analysis and the subsequent memo and articles based on his work. There are only documents and file archives that purport to have been extracted from DNC storage in 2016 along with the metadata contained within them. The metadata includes "Last Modified" timestamps at various levels of time resolutions (milliseconds, nanoseconds) that also include time-zone information.

Otherwise, there are no logs available that would provide an audit trail of network or system activity. There is no public copy of malicious software found on a targeted system that can be decompiled, reverse engineered, and analyzed. There is no information about where or how the extracted files were stored, what the operating systems involved were, or what the local, co-located, or hosted network configuration and speed might have been.

Most of this document focuses on the findings related to throughput. It also includes a brief set of findings related to the issue of revision save identifiers (RSIDs) and their role in tracking the edit history of word-processing documents.

Time Gaps and Throughput: The Forensicator proposes that all the files in the archive were copied in a single batch operation, and that time gaps in the file and archive metadata indicate that some copied files were not included in the final public archive. By removing the time those missing files would have taken to be copied from the total difference of time from newest to oldest in the archive, the Forensicator arrives at a specific total transfer time of 87 seconds. By then dividing the total size of the archive by that time, he arrives at the calculation of 23 megabytes per second (the amount of megabytes of data that could be transferred over a network or between storage drives per second).

In a recent comment, the Forensicator simplified his throughput theory by reducing the set of files the time estimate is generated from: "There is a series of files and directories that have no time gaps: it includes some top-level files and the FEC directory. The total size is 869 MB, which is 40% of the total. Using only the earliest last mod time and the latest in that series of files, the total elapsed time is 31 seconds. The transfer rate for those files works out to 28 MB/s."

Nontechnical readers can be forgiven for not firmly grasping the difference between megabytes per second and megabits per second. The overall point of this portion of the analysis was to understand the kind of digital transfer speeds that were utilized by the adversary when extracting the files from the DNC computing resources. The Forensicator ultimately only provides a "right ballpark" number of

23 megabytes per second; that is enough to simply state that a high amount of sustained throughput was utilized during the copying of the files provided. Twenty-three megabytes per second (MB/s) translates to roughly 184 megabits per second (Mb/s).

While most home-network Internet service providers in the United States theoretically offer 100-megabits-per-second download speeds (and some such as Google Fiber offer higher), they rarely reach that full speed and definitely not speeds of up to 184Mb/s. However, that throughput could be achieved by a variety of other digital-communication configurations: a high-speed business-grade Internet service provider, an intra-office local area network, communication between servers within a commercial cloud provider or between high-availability data centers, or over a universal serial bus (USB) connection to an external storage device.

Claims Without Data: Lawrence's article makes the following statement: "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."

The VIPS memo makes the following statement: "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."

The only accurate portion of these statements, backed by metadata from the files and archive, is the total size of 1,976 megabytes. As stated before, the transfer time of 87 seconds is an informed theory by the Forensicator, and the 22.7-megabytes-per-second transfer rate is built upon that theory, along with some other educated guesses. While the "Last Modified" value of the files do indicate a copy operation occurred on July 5, 2016, and while the time zone does indicate the computing resources participating in the copy were set to Eastern Standard Time, there is no metadata showing they were downloaded from any specific server, on any specific network, or in any specific geographic location. Finally, the claim that 22.7 megabytes per second is "much faster than what is physically possible with a hack" needs to be addressed in greater depth.

Many Ways to 23 Megabytes per Second: Let us consider the "remote hacker" in this situation. The adversary in a remote intrusion can be physically located nearly anywhere in the world. They can be multiple people working in coordination, in control of a vast amount of physically diverse computing resources through vast networks of compromised machines (also known as “botnets”). They can also utilize a wide variety of network communication tunnels, proxies, and virtual private networks to mask their traffic and true network address. If this remote adversary was attempting to directly copy data from the compromised target server to their actual physical location, a very difficult-to-achieve high sustained throughput would be required to match the time-stamp metadata in the files.

But if the remote adversary was directly downloading the files from the target server to a temporary cloud server or otherwise compromised third-party server within close network proximity, that throughput speed would be possible to achieve. The cloud server could have been provided by a system like Microsoft Azure or Amazon Web Services (AWS), which provide computing resources in the Eastern United States. Creating disposable server instances on cloud services like AWS is easy, cheap, and achievable with relative anonymity. The adversary’s remote-control connection to the cloud could have been slowed by multiple hops through tunnels and VPNs, but the connection between the cloud server itself and the target server need not be.

Another scenario that would more precisely match the 23-megabytes-per-second transfer rate is that of an end-user workstation on the local area network being compromised by a remote-access Trojan (RAT). This scenario has also been called “the local pivot.” The compromise would occur through an e-mail-phishing or document-attachment malware attack on a staff member operating the workstation. These attacks are extremely common and easy to execute. RATs provide full “remote control” over an infected target system. Data exfiltration via phished malware is something that has been happening for at least a decade, as proven by the 2009 GhostNet attack against the Tibetan government in exile and others.

If the attack is successful, the RAT would run on the internal workstation, which was likely running Windows 7, with a primary disk formatted as NTFS and another local storage disk formatted in FAT32. The specifics of the file-system formats matter when it comes to matching the format of time stamps analyzed by the Forensicator. This machine would have been connected to the local area network and would have had access to a file-sharing server (likely “Samba” or Windows SMB-based) from which the documents were copied. The RAT would utilize the authenticated user it compromised to invisibly access the files over the local area network, copy them in bulk to the local machine at 23 megabytes per second, and package them into an archive for remote transfer. The metadata matching the Forensicator’s analysis would have been fully generated at this point. The final copy to the remote adversary's source machine could happen at any speed.

These are just two scenarios that could generate the file archive necessary to match the Forensicator's findings. They are as much based on informed theories and educated guesses as the scenarios proposed by the Forensicator, the VIPS memo, and Lawrence's article. While some may feel the simplest answer is always the most likely, the two alternate scenarios described above are common enough that they should be considered plausible. In either scenario, the adversary need neither be a state actor nor require an unusual amount of resources.

The Forensicator's Leaker Boot-Drive Theory: Another way to reach the 23-megabytes-per-second speed is through a mass copy of files either from a local machine's hard drive or a connected local network file server, such as in the RAT scenario, to an attached USB thumb or "flash" drive. This is the method proposed by the Forensicator in his analysis: "A Linux OS may have been booted from a USB flash drive and the data may have been copied back to the same flash drive, which will likely have been formatted with the Linux (ext4) file system."

This last step is necessary to the leaker boot-drive theory—rather than just a standard drag-and-drop of files into an attached USB—because the

Forensicator's analysis of the metadata time-stamp changes shows that the copy operation was done by a "cp" command-line call typical of a Linux system. It is important to note that it is unclear why the alleged internal leaker would need to reboot into Linux in this manner if the leaker already had authorized access to the system and files in question. Additionally, necessitating the leaker to reboot into Linux raises other difficulties. If the documents were stored on a network file share, access to it would be secured and require authorized credentials. If the machine is rebooted out of Windows and into Linux, then there is no authenticated user on the machine. The alleged leaker's Linux OS would need authenticated credentials in order to access the server file share. This means that there would be a record of the authenticated access on the target server, or of a compromised access from an internal network source.

The final complexity with the local-leaker theory is that the 23-megabytes-per-second rate is based on an assumption that the files are on the local machine or on a server in the local area network. If the argument that 23 megabytes per second would not be possible by a remote adversary is the key finding, then the local leaker would also have to have that level of throughput available. The target server, then, would need to be physically on site in the building—and not hosted in a remote data center. If the files were stored remotely "in the cloud," then the same criticism of "it is not possible to get those speeds" would come into play, as the local desktop with the booted Linux OS would now essentially be a remote hacker's PC.

Unfortunately, as stated at the beginning of this review, there has been little information shared about the location and configuration of networks, servers, and other DNC infrastructure.

On "Russian Fingerprints": In a timeline on the g-2.space site, Adam Carter provides this entry for June 15, 2016:š
"Someone choosing to adopt the name of hacker recently in the news *('Guccifer', whom [*sic*] was in court the previous month)*, steps forward, calling himself Guccifer2.0 and claiming responsibility for the hack. He affirms the DNC statement and claims to be a source for Wikileaks. The first 5 documents he posts are purposefully tainted with 'Russian Fingerprints' and the first of those documents just so happens to be the **'Trump Opposition Research'** the DNC announce on the previous day."

The claim regarding "Russian Fingerprints" concerns a number of things, including the name the document author was set to, the type of keyboard used to edit the comments, and the existence of shared language style settings in multiple documents. It is accurate that the documents provided by

"Guccifer 2.0" all contain the same revision-save identifier (RSID) related to a Russian-language style change.

The existence of identical revision-save identifiers within a Microsoft Word or Rich Text Format document indicates that the set of documents was created from a shared source. This shared lineage can occur when starting with a single formatted document template, or it can occur when copying and pasting a piece of content into multiple files. As discussed in this article [PDF], RSIDs can be used to detect plagiarized academic papers. Inspecting RSIDs can detect if students copy from each other, or from a previously submitted paper from an earlier year, for example. If multiple documents contain the same RSID, it means they have a shared lineage. It could mean they all came from one document that was copied and pasted into three documents. It could also mean that a small piece, say a header or appendage text, was copied from one document into the others. There are many ways RSIDs can end up being shared between multiple documents.

As in the case of the Forensicator's throughput analysis, there is a kernel of accuracy in the "Russian Fingerprints" theory backed by the metadata in the documents. The documents provided by "Guccifer 2.0" show that they were created or edited through a process that caused them to have, in some small part, a shared document lineage. This lineage included markers related to encoding of data in the Russian language.

There is nothing in the metadata, however, to indicate the motivations of "Guccifer 2.0" or whoever created these modified documents. The fact that the documents provided were named with simple numbers in a sequential order (1.doc, 2.doc, etc.) could indicate that "Guccifer 2.0" was attempting to curate and edit content and not simply dumping exact copies of the same documents provided elsewhere. The fact that the documents were also saved as Rich Text Format shows that there was an attempt to format files in a "clean" state, and not simply share the original source files.

Conclusion: Good-faith efforts to parse the available data to provide insight into the unlawful extraction of documents from the DNC in 2016 are admirable and necessary. All parties, however, must exercise much greater care in separating out statements backed by available digital metadata from thoughtful insights and educated guesses. Walking nontechnical readers down any narrative path that cannot be directly supported by evidence must be avoided. At this point, given the limited available data, certainty about only a very small number of things can be achieved.

Various Contributors

To submit a correction for our consideration, click *here*.
For Reprints and Permissions, click *here*.

COMMENTS (23)

JAILS AND PRISONS STATE AND LOCAL ELECTIONS MASS INCARCERATION

Philadelphia Just Elected the Most Radical DA in the Country—Now What?

Larry Krasner has pledged to fight mass incarceration, and activists say they'll be watching.

By Daniel Denvir

TODAY 1:08 PM

Larry Krasner walks from his polling place in Philadelphia, Tuesday, November 7, 2017. *(Associated Press / Matt Rourke)*

On Tuesday, Philadelphians elected Larry Krasner to be their district attorney. Krasner, a long-time civil rights lawyer and critic of mass incarceration, is a frequent litigant against abusive cops and boasts a list of rabble-rousing clientele including activists from Black Lives Matter and Occupy Philly. He was propelled into office by an energized left coalition led by youth and people of color. Their organizing work boosted turnout by at least 69-percent compared to the city's last DA's race.

Even as President Trump fulminates against immigrant gangsters and Attorney General Sessions endeavors to reinvigorate the failed "war on crime," voters have elected a candidate who has said he wants to "end the era of mass incarceration." It's an enormous task. Since the 1970s, American policing and prisons have metastasized: at the end of 1980, state prisons held 304,844 people, but by the end of 2015, they held more than 1,330,000. The country's entire system of cages, which includes everything from federal prisons to immigrant detention centers, incarcerates more than 2.3 million. Incarceration rates began to decline in 2010, but reducing prison populations to levels comparable to, say, those of Western Europe, will require big changes. Thd policing and prosecuting practices that filled our prisons are deeply ingrained in the day-to-day practices of the criminal justice system.

One path forward has been presented by the Coalition for a Just District Attorney, comprising nearly 30 local groups, in their just-released "Vision Of Transformative Policies" for Krasner's first 100 Days. Their agenda includes ending civil asset forfeiture, a shameful program allowing police to seize people's property before they were convicted of a crime (Krasner's Republican opponent had overseen this program during her time in the DAs office). It also demands that Krasner decline to prosecute many "quality of life" offenses, from drug possession to prostitution; bring the office's moribund Conviction Review Unit to life so that it keeps the wrongfully convicted out of prison; take into account whether filing certain charges would increase an immigrant's risk of deportation; cease to deal with police officers with track records of misconduct; and adopt an open file system for pre-trial discovery, so that defense lawyers have immediate access to the information that prosecutors will use against their clients.

Krasner has not yet issued a full response to this lengthy list of proposals. But he ran on a pledge to divert low-level offenses from the criminal justice system, crack down on prosecutor complicity with police misconduct, and right wrongful convictions. It won't all, of course, be easy. He must confront possible resistance from DA office veterans, whom he can fire, and from cops, whom he cannot (though he can and should prosecute them, of course, if they break the law).

Krasner has also pledged to stop seeking the death penalty. That's a good thing. But Pennsylvania has only executed three people since 1962. The best thing about formally ending the death penalty is that it will allow us to stop talking about the death penalty and focus on the drivers of mass incarceration.

Krasner wants to end cash bail, one essential step in decreasing the number of people behind bars. Cash bail is a patently unjust system that keeps people in jail pending trial based on whether or not they have sufficient financial resources, rather than on whether they might pose a threat to public safety or a flight risk. Reducing the number of people held on bail will help. Roughly 25 percent of those held in city jails, known as the Philadelphia Prison System, are held on bail pending trial, according to the city. Formally ending cash bail won't be easy because doing so would require the cooperation of Pennsylvania's Republican-controlled state legislature. But Krasner believes that he can work toward putting an end to the system *in effect* by directing prosecutors to request that magistrates release anyone who should not be detained on their own recognizance, and requesting astronomical bail for people if they should. That too, however, will require the cooperation of the Philadelphia court system.

Philadelphia has already made some progress toward reducing incarceration, collaborating with the MacArthur Foundation to reduce the city jail population by 34 percent. The current city jail population is roughly 6,729, a 17-percent decrease from the 8,082 locked up in July 2015. A deep reduction in Pennsylvania's incarcerated population will require fewer people held on cash bail. Reducing it further than that will require digging yet deeper. Many held in city jails are there because of technical parole and probation violations. Many of them could be kept out of the system in the first place. But that will likely require the cooperation of the city courts as well. What's more, roughly one-in-five in city jails are serving short sentences of 23 months or less. Arguably, many of those sentenced to such short stints behind bars don't need to be there in the first place.

What's more daunting, perhaps, is that 13,576 people from Philadelphia were locked up in state prisons as of the end of 2016— a gargantuan system that cages city residents in far-flung facilities as far as a full-day's car ride, or an overnight bus-trip, from the city —with 1,694 newly sent from city courts, and another 1,844 for parole violations, last year alone. New Philadelphia court commitments to state prisons declined by 11.4-percent between 2015 and 2016. But bringing those numbers down more dramatically will require reforms beyond ceasing to prosecute small-time quality-of-life offenses.

Prison populations are governed by a simple equation: how many people are sent to prison multiplied by how many years and months they are sentenced to serve. According to the state Department of Corrections, that number sent to state prison in 2016 included 303 for drug crimes, 270 for robbery, 138 for murder, 289 for aggravated assault, and 293 on weapons offenses. Reducing Philadelphia's contribution to mass incarceration thus will require not only the justice system declining to send some to prison in the first but also sentencing those who are sent away to prison to less time.

"This notion that people are either all bad or all good is untrue and these changes in criminal justice are going to demonstrate that," says Krasner. "And there's going to be a more balanced and reasonable view of what you do with people in cases that we all view as non-serious, and even what you do in cases that are a little bit more serious but appear to be situational, age-related, related to prior trauma, things of that sort, which make it clear that people are not permanently that way."

Krasner, however, said that "no one seems to be really pushing the idea of getting back to the 1970s levels." I asked him what it would take to do start having that conversation.

"We can think about it," Krasner responded. "But we also have to deal with political realities." If early reductions go well "not only well in terms of actual statistics, but well in terms of how that narrative is handled by a press, then I think everybody will be much more open." But if the typical sensationalist narratives about crime prevail, a "stupid narrative about how one bad result negates all the good results…it will be very difficult to have the buy-in."

Krasner will likely fall short of the expectations set by the activists who propelled him into office—at the end of the day, his job will involve sending people to prison, while many activists would like to see the prison system destroyed altogether. Both Krasner and his supporters agree that dialogue will be key. Sheila Quintana, a community organizer for the New Sanctuary Movement of Philadelphia, a member of the coalition, says that they are ready to fight for Krasner. And also to fight for their agenda. To make sure that Krasner follows through, they want data on all cases to be made fully public, and quarterly meetings to evaluate progress. "We want a collaborative relationship," says Quintana. "We know that Krasner's going to have a difficult time coming into the prosecutor's office…we want to support him so that we can actually accomplish the things that we need accomplished…but of course, continuing to push when necessary for the changes to happen."

Daniel Denvir Daniel Denvir is a fellow at Harvard Law School's Fair Punishment Project and the host of The Dig, a podcast from Jacobin magazine.

To submit a correction for our consideration, click *here*.
For Reprints and Permissions, click *here*.

COMMENTS (0)