

Der ehemalige NSA-Mitarbeiter William Binney und der ehemalige CIA-Analyst Ray McGovern haben durch zusätzliche Tests ihre Schlussfolgerung erhärtet, dass die E-Mails aus den Computern der Demokratischen Partei nicht von Russen "gehackt", sondern von einem Insider direkt heruntergeladen, also "geleakt" wurden.

LUFTPOST

**Friedenspolitische Mitteilungen aus der
US-Militärregion Kaiserslautern/Ramstein
LP 166/17 – 16.10.17**

**Noch mehr Löcher in der Mür über die russischen Hacker
Exklusiv: Neue Tests stützen die Zweifel ehemaliger Mitarbeiter von US-Geheimdiensten an der Behauptung, "russische Hacker" seien in die Computer des DNC eingedrungen; sie bestätigen hingegen die Annahme, dass ein Insider die E-Mails direkt heruntergeladen hat. Das schreiben der ehemalige NSA-Mitarbeiter William Binney und der ehemalige CIA-Analyst Ray McGovern.**

Von William Binney und Ray McGovern
Consortiumnews.com, 20.09.17

(<https://consortiumnews.com/2017/09/20/more-holes-in-russia-gate-narrative/>)

Es ist kein Geheimnis, dass unser VIPS-Memorandum mit der Überschrift "Was the 'Russian Hack' an Inside Job?" (War der „russische Hackerangriff“ ein Inside-Job?, s. http://www.luftpost-kl.de/luftpost-archiv/LP_16/LP12617_310717.pdf), das wir am 24. Juli an den US-Präsidenten gerichtet haben, einige Fragen aufgeworfen und eine Kontroverse ausgelöst hat; es hat uns auch nicht überrascht, dass die Mainstream-Medien kaum darüber berichtet haben.

Die immer noch andauernde Kampagne, die in den US-Medien gegen Russland inszeniert wurde, ist so wirksam, dass sogar intelligente Menschen nicht erkennen wollen, dass sie von den US-Geheimdiensten vollkommen in die Irre geführt werden. Das geschah zuletzt im Jahr 2003, als nach einer ähnlichen Propagandakampagne, die ein ganzes Jahr lief, die USA auf Grund bewusst gefälschter – nicht etwa "falsch interpretierter" – geheimdienstlicher Erkenntnisse den Irak überfallen haben.

Wohl wissend, dass Leute, welche die Mür von der "russischen Einmischung" (in die Wahl des US-Präsidenten) deshalb für wahr halten, "weil sie allgemein bekannt ist", allergisch auf unsere VIPS-Analyse reagieren würden, haben wir diese Analyse nur auf forensische Untersuchungen gestützt, die das FBI vorsätzlich nicht durchgeführt hat. Mit anderen Worten, wir haben uns nur auf die Gesetze der Physik und die Möglichkeiten verlassen, die Anfang Juli 2016 im Internet zur Verfügung standen.

Wir bleiben bei unserer Hauptschlussfolgerung, dass die Daten, die am 5. Juli 2016 aus den Computern des Democratic National Committee's / DNC (s. dazu auch https://de.wikipedia.org/wiki/Democratic_National_Committee), gestohlen wurden, nicht von "russischen Hackern" (die über das Internet in die Computer eingedrungen sein sollen) entwendet, sondern von einer Person, die direkten Zugang zu den Computern hatte, als Kopie auf ein externes Speichermedium heruntergeladen wurden.

Diese grundlegende Erkenntnis beruht auf der Geschwindigkeit, in der die Kopie angefertigt wurde; das Herunterladen erfolgte nämlich viel schneller, als es damals über das Internet möglich gewesen wäre und – auch das scheint jetzt klar zu sein – sogar heute noch möglich wäre. Weil unsere Schlussfolgerung von Leuten angezweifelt wurde, die sie unter eingeschränkten Laborbedingungen überprüften, haben wir zusätzliche Tests durchgeführt

und dokumentiert, um die Übertragungsgeschwindigkeiten zu bestimmen, die jetzt – mehr als ein Jahr später – erreicht werden können.

Zur Erinnerung: In unserem VIPS-Memorandum vom 5. Juli 2016 haben wir dargelegt, dass von einem Computer, der direkt mit dem DNC-Server oder einem lokalen DNC-Netzwerk verbunden war, eine Datenmenge von 1.976 Megabytes in 87 Sekunden auf ein externes Speichermedium kopiert wurde. Das ergibt eine Übertragungsgeschwindigkeit von 22,7 Megabytes pro Sekunde.

Neue Tests

In den letzten Wochen haben wir drei Tests durchgeführt, um herauszufinden, wie schnell Daten aus den USA über den Atlantik nach Europa übertragen werden können.

Erstens haben wir mit einer Leitung, die 100 Megabytes pro Sekunde / Mbps transportieren kann, eine Datei von 1 Gigabyte nach Amsterdam geschickt. Die maximale Übertragungsgeschwindigkeit betrug 0,8 Mbps.

Zweitens haben wir die gleiche 1-Gigabyte-Datei über eine kommerzielle Digital Subscriber Line / DSL nach Amsterdam gesandt. Die maximale Übertragungsgeschwindigkeit betrug 1,8 Mbps.

Drittens haben wir die gleiche 1-Gigabyte-Datei von einem Datenzentrum in New Jersey zu einem Datenzentrum in Großbritannien weitergeleitet. Die maximale Übertragungsgeschwindigkeit betrug 12 Mbps.

Bei keinem dieser Versuche kamen wir auch nur in die Nähe einer durchschnittlichen Übertragungsgeschwindigkeit von 22,7 Megabytes pro Sekunde, mit der am 5. Juli 2016 die Kopie aus den DNC-Computern heruntergeladen wurde. Die Übertragungsgeschwindigkeit von 22,7 Mbps ist aber typisch für die Datenübertragung auf einen USB-2-Stick. Das halten wir nicht für einen Zufall, wir betrachten das als zusätzlichen Beweis dafür, dass die gestohlenen E-Mails direkt vor Ort auf einen solchen Datenstick heruntergeladen wurden.

In den kommenden Wochen wollen wir weitere transatlantische Tests durchführen.

Einige Experten haben vermutet, die große Datenmenge sei vorher in den USA geteilt worden, um eine höhere Übertragungsgeschwindigkeit zu ermöglichen und Hackern auf der anderen Seite des Atlantiks den Zugriff zu erleichtern. Einer der mit uns zusammenarbeitenden Fachleute hat festgestellt, dass diese Möglichkeit bestünde.

Theoretisch könnten auf diese Weise größere Datenmengen in kürzerer Zeit übertragen werden, es gibt aber keine Beweise dafür, dass das tatsächlich auch geschehen ist. Noch wichtiger ist, dass die NSA das hätte bemerken müssen, weil für die Teilung von Daten vor der Übertragung eine spezielle Software erforderlich ist und die NSA vorrangig nach derartiger "Ausführungssoftware" sucht.

Müssen die US-Bürger einschließlich ihres Präsidenten Donald Trump also weiterhin glauben, dass es "die Russen waren oder wenigstens gewesen sein könnten", oder wurde diese Mär nur verbreitet, um die Beziehungen zu Russland zu einem neuen Kalten Krieg zu vereisen? Die US-Bürger dürfen diese Mär jetzt auf keinen Fall immer noch glauben, denn wir haben schlüssig nachgewiesen, dass sie nicht stimmen kann.

Wie können wir uns dessen so sicher sein? Weil frühere NSA-Mitarbeiter, die jetzt zu den Veteran Intelligence Professionals for Sanity / VIPS (den Ehemaligen Mitarbeitern von US-Geheimdiensten für Vernunft) gehören, mit den Fähigkeiten der NSA und ihrer Praxis zur Überwachung und Speicherung der über Glasfaserkabel abgewickelten Kommunikation vertraut sind. Zwei von uns haben bei der Einrichtung der noch genutzten Überwachungssysteme mitgewirkt, und die Enthüllungen Edward Snowdens haben inzwischen entstandene Lücken ausgefüllt. Die NSA ist heute in der Lage, alle im Zusammenhang mit irgendwelchen Hacker-Angriffen auf die DNC-Computer stehenden Fragen lückenlos aufzuklären.

Wir sind also absolut sicher, dass die Wahrheit über tatsächliche oder angebliche Hacker-Angriffe in den Datenbanken der NSA gefunden werden kann. In einem VIPS-Memorandum vom 17. Januar 2017 [s. <https://consortiumnews.com/2017/01/17/a-demand-for-russian-hacking-proof/>] haben wir versucht, den Präsidenten Barack Obama noch drei Tage vor dem Ende seiner Amtszeit darauf hinzuweisen, dass die NSA mit ihren bekannt gewordenen Programmen und in Zusammenarbeit mit verbündeten Geheimdiensten dazu fähig ist, alle elektronischen Datenübermittlungen zu erfassen.

Unser Memorandum vom 17. Januar enthielt auch folgende Empfehlung: "Wir bitten Sie dringend, die NSA um die Vorlage von Beweisen dafür zu ersuchen, dass russische Hacker Ergebnisse ihrer Angriffe an WikiLeaks weitergegeben haben. ... Wenn die NSA Ihnen nicht schnellstens solche Beweise liefern kann, bedeutet das vermutlich, dass sie keine hat."

In den letzten Tagen seiner Amtszeit haben wir außerdem an Obama appelliert, die Chefs der NSA, des FBI und der CIA ins Weiße Haus einzubestellen und sie alle aufzufordern, ihre sämtlichen Karten über "russische Hacker" auf den Tisch zu legen, also handfeste Beweise zu präsentieren und nicht nur mit "Einschätzungen" zu operieren. Wir fügten hinzu: "Wir hoffen doch sehr, dass Sie Ihrem Nachfolger keine Anschuldigungen hinterlassen werden, die keiner Überprüfung standhalten." Schon damals gingen wir davon aus, dass es keine belastbaren Beweise für die "Einschätzungen" (der US-Geheimdienste) gegeben hat.

Auch das FBI hat versagt

Das FBI könnte auch heute noch nachholen, was es versäumt hat, als der DNC behauptete, seine Computer seien "gehackt" worden. Aus irgendwelchen Gründen, die nur der damalige FBI-Direktor James Comey kennt, hat man sich damals keine Genehmigung besorgt, die man gebraucht hätte, um die DNC-Server und Computer beschlagnahmen und überprüfen zu können.

Vor sechs Monaten hat Comey in einer Anhörung vor dem Geheimdienstausschuss des Repräsentantenhauses ausgesagt: "In solchen Fällen ist es immer am besten, die betroffenen Geräte zu untersuchen." Das hat er aber nicht veranlasst, obwohl Russland damals von führenden US-Offiziellen lautstark beschuldigt wurde, "eine Kriegshandlung" begangen zu haben.

Wäre es heute zu spät für eine solche Untersuchung? Wir glauben, dass es noch nicht zu spät ist. Alle Daten, die das FBI bräuchte, um sein Versäumnis wieder gut zu machen, befinden sich in den NSA-Datenbanken – einschließlich der Daten, die über das Internet zum DNC-Server gegangen und auf dessen Netzwerk eingewirkt haben sollen.

Wenn Präsident Trump die Wahrheit wissen will, muss er dem FBI befehlen, seinen Job zu machen, und anordnen, dass die NSA dabei mit ihm kooperiert. Ob ihm das FBI, die

NSA und eventuell auch die CIA gehorchen würden, ist eine offene Frage, weil alle drei eifrig an der unhaltbaren Mär von den "russischen Hackern" mitgestrickt haben.

Wiederholen wir das Offensichtliche: Die Bundespolizei und die beiden Geheimdienste wussten schon die ganze Zeit, dass die NSA alle Daten gespeichert hat. Man fragt sich, warum der Präsident überhaupt eine auf Fakten und nicht auf "Einschätzungen" beruhende Untersuchung anordnen muss.

William Binney (williambinney0802@comcast.net) hat 36 Jahre lang für die NSA gearbeitet, bis er 2001 als Technischer Direktor für globale militärische und geopolitische Analysen in den Ruhestand ging; er hat viele der auch heute noch von der NSA verwendeten Überwachungssysteme mitgeschaffen. Ray McGovern (rrmcgovern@gmail.com) war 27 Jahre lang CIA-Analyst und hat von 1981 bis 1985 den damaligen US-Präsidenten Reagan täglich über aktuelle geheimdienstliche Erkenntnisse informiert.

(Wir haben den Artikel komplett übersetzt und mit Ergänzungen und Links in runden Klammern versehen. Den Link in eckigen Klammern haben die Autoren selbst eingefügt. Damit dürfte die Mär von den "russischen Hackern" endgültig als Lügenstory entlarvt sein. Anschließend drucken wir den Originaltext ab.)



More Holes in Russia-gate Narrative

Exclusive: New tests support the skepticism of U.S. intelligence veterans that Russia “hacked” the DNC’s computers, pointing instead to a download of emails by an insider, write ex-NSA official William Binney and ex-CIA analyst Ray McGovern.

By William Binney and Ray McGovern, September 20, 2017

It is no secret that our July 24 VIPS Memorandum for the President, entitled “Was the ‘Russian Hack’ an Inside Job?,” gave rise to some questioning and controversy – nor was it a surprise that it was met with almost total silence in the mainstream media.

The ongoing U.S. media campaign against Russia has been so effective that otherwise intelligent people have been unable even to entertain the notion that they may have been totally misled by the intelligence community. The last time this happened in 2003, after a year of such propaganda, the U.S. attacked Iraq on fraudulent – not “mistaken” – intelligence.

Anticipating resistance from those allergic to rethinking “what everybody knows” about Russian “meddling,” we based our VIPS analysis on forensic investigations that, oddly, the FBI had bent over backwards to avoid. In other words, we relied on the principles of physics and the known capability of the Internet in early July 2016.

We stand by our main conclusion that the data from the intrusion of July 5, 2016, into the Democratic National Committee’s computers, an intrusion blamed on “Russian hacking,” was not a hack but rather a download/copy onto an external storage device by someone with physical access to the DNC.

That principal finding relied heavily on the speed with which the copy took place – a speed much faster than a hack over the Internet could have achieved at the time – or, it seems clear, even now. Challenged on that conclusion – often by those conducting experiments within the confines of a laboratory – we have conducted and documented additional tests to determine the speeds that can be achieved now, more than a year later.

To remind: We noted in the VIPS memo that on July 5, 2016, 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 yields a transfer rate of 22.7 megabytes per second.

Recent Tests

Over the last few weeks, we ran three tests to determine how quickly data could be exfiltrated from the U.S. across the Atlantic to Europe.

–First, we used a 100 megabits-per-second (mbps) line to pull data from a one-gigabyte file to Amsterdam. The peak transfer speed was .8 MBps.

–Second, we used a commercial DSL (Digital Subscriber Line) to send the same one-gigabyte file to a commercial DSL in Amsterdam. The peak transfer speed was 1.8 MBps.

–Third, we pushed the same one-gigabyte file from a data center in New Jersey to a data center in the UK. The peak transfer speed was 12 MBps.

None of these attempts achieve anything close to the average rate of 22.7 megabytes per second evident in the July 5, 2016 download/copy associated with the DNC. In fact, this happens to be the speed typical of a transfer to a USB-2 external storage device. We do not think this pure coincidence; rather, it is additional evidence of a local download.

We are preparing further trans-Atlantic testing over the next few weeks.

Some researchers have noted that some partitioning of the data might have occurred in the U.S., allowing for a transfer to be made at the measured speed over the Internet, and that this could have made possible a hack from the other side of the Atlantic. One of our associate investigators has found a way to achieve this kind of data partitioning and later transfer.

In theory, this would be one possible way to achieve such a large-data transfer, but we have no evidence that anything like this actually occurred. More important, in such a scenario, the National Security Agency would have chapter and verse on it, because such a hack would have to include software to execute the partitioning and subsequent data transfer. NSA gives the highest priority to collection on “execution software.”

Must Americans, apparently including President Donald Trump, remain in a Russia-did-it-or-could-have-maybe-might-have-done-it subjunctive mood on this important issue – one that has been used to inject Cold War ice into relations with Russia? The answer is absolutely not. Rather, definitive answers are at hand.

How can we be so confident? Because NSA alumni now active in Veteran Intelligence Professionals for Sanity (VIPS) are intimately familiar with NSA’s capabilities and practice with respect to bulk capture and storage of fiber-optic communications. Two of us actually devised the systems still in use, and Edward Snowden’s revelations filled in remaining gaps.

Today's NSA is in position to clear up any and all questions about intrusions into the DNC.

In sum, we are certain that the truth of what actually happened – or didn't happen – can be found in the databases of NSA. We tried to explain this to President Barack Obama in a VIPS Memorandum of Jan. 17, just three days before he left office, noting that NSA's known programs are fully capable of capturing – and together with liaison intelligence services do capture – all electronic transfers of data.

Our Jan. 17 Memorandum included this admonition: "We strongly suggest that you ask NSA for any evidence it may have indicating that the results of Russian hacking were given to WikiLeaks." ... "If NSA cannot give you that information – and quickly – this would probably mean it does not have any."

We also appealed to Obama in his final days in office to order the chiefs of the NSA, FBI and CIA to the White House and have them lay all their cards on the table about "Russian hacking," and show him what tangible evidence they might have – not simply their "assessments." We added, "We assume you would not wish to hobble your successor with charges that cannot withstand close scrutiny." Having said this, we already were reaching the assumption that there was no real evidence to back the "assessments" up.

FBI: Not Leaning Forward

The FBI could still redeem itself by doing what it should have done as soon as the DNC claimed to have been "hacked." For reasons best known to former FBI Director James Comey, the Bureau failed to get whatever warrant was needed to confiscate the DNC servers and computers to properly examine them.

In testimony to the House Intelligence Committee six months ago, Comey conceded "best practice is always to get access to the machines themselves." And yet he chose not to. And his decision came amid frenzied charges by senior U.S. officials that Russia had committed "an act of war."

But is it not already too late for such an investigation? We hope that, at this point, it is crystal clear that the answer is: No, it is not too late. All the data the FBI needs to do a proper job is in NSA databases – including data going across the Internet to the DNC server and then included in their network logs.

If President Trump wants to know the truth, he can order the FBI to do its job and NSA to cooperate. Whether the two and the CIA would obey such orders is an open question, given how heavily invested all three agencies are in their evidence-impooverished narrative about "Russian hacking."

Let us close with the obvious. All three agencies have been aware all along that NSA has the data. One wonders why it should require a Presidential order for them to delve into that data and come up with conclusions based on fact, as opposed to "assessing."

William Binney (williambinney0802@comcast.net) worked for NSA for 36 years, retiring in 2001 as the technical director of world military and geopolitical analysis and reporting; he created many of the collection systems still used by NSA. Ray McGovern (rrmcgovern@gmail.com) was a CIA analyst for 27 years; from 1981 to 1985 he briefed the President's Daily Brief one-on-one to President Reagan's most senior national security officials.