Ehemalige Mitarbeiter von US-Geheimdiensten haben in einem Memorandum an den US-Präsidenten Donald Trump nachgewiesen, dass die E-Mails der Demokraten nicht von "russischen Hackern" öffentlich gemacht wurden.

LUFTPOST

Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein
LP 126/17 – 31.07.17

Ehemalige Mitarbeiter von US-Geheimdiensten stellen die "Wahlbeeinflussung durch russische Hacker" infrage

In einem Memorandum an den Präsidenten Trump weist eine Gruppe ehemaliger Mitarbeiter von US-Geheimdiensten, darunter auch NSA-Experten, unter Berufung auf neue forensische Studien die in der "Bewertung" vom 6. Januar aufgestellte Behauptung, Russland habe 2016 E-Mails der Demokraten "hacken" lassen, als nicht haltbar zurück.

Consortiumnews.com, 24.07.17
(https://consortiumnews.com/2017/07/24/intel-vets-challenge-russia-hack-evidence/)

Die nachfolgend abgedruckte Übersetzung haben wir inhaltlich unverändert übernommen aus https://deutsch.rt.com/nordamerika/54668-us-geheimdienstveteranen-es-gab-keinen-russischen-hackerangriff-us-wahlen/ . Die Links in eckigen Klammern waren bereits im Originaltext enthalten.

Memorandum an den US-Präsidenten

Von den Veteran Intelligence Professionals for Sanity (VIPS)

Betrifft: War der „russische Hackerangriff“ ein Inside-Job?

Kurzfassung

Forensische Studien zu dem „russischen Hackerangriff“ auf Computer des Nationalen Komitees der Demokraten (NC) im vergangenen Jahr zeigen, dass am 5. Juli 2016 Daten von einer Person mit physischem Zugang zu den DNC-Computern geleakt (nicht gehackt) wurden, die anschließend manipuliert wurden, um Russland belasten zu können.

Nach der Untersuchung von Metadaten des „Guccifer 2.0“ Angriffs vom 5. Juli 2016 auf den DNC-Server haben unabhängige Cyber-Ermittler festgestellt, dass ein Insider Daten auf ein externes Speichergerät kopierte und dass anschließend „verräterische Spuren“ eingefügt wurden, die auf Russland hinweisen. Die unabhängige forensische Untersuchung kam zu dem Ergebnis, dass die DNC-Daten mit einer Geschwindigkeit auf ein Speichergerät kopiert wurden, die die Verbindungskapazitäten des Internets weit übersteigt, die bei einem Hackerangriff von außen erforderlich wären.

Die Untersuchung zeigt zudem, dass der Kopiervorgang und die Datenmanipulation von der Ostküste der USA aus durchgeführt wurden. Bisher haben die Mainstream-Medien die Ergebnisse dieser unabhängigen Studien ignoriert [s. dazu auch http://disobedientmedia.com/2017/07/new-research-shows-guccifer-2-0-files-were-copied-locally-not-hacked/ und https://theforensicator.wordpress.com/guccifer-2-ngp-van-metadata-analysis/].

Der unabhängige Analyst Skip Folden, ein pensionierter IBM-Programmmanager für Informationstechnologie, der die jüngsten forensischen Befunde untersuchte, hat dieses Me-

morandum mit verfasst. Er hat einen ausführlicheren Bericht mit technischen Details unter dem Titel „Cyber-Forensic Investigation of ‚Russian Hack' and Missing Intelligence Community Disclaimers" verfasst und diesen an die Büros des Sonderermittlers und des Justizministers geschickt. Neben William Binney, ehemaliger Technischer Direktor der National Security Agency, haben andere hochrangige ehemalige Mitarbeiter der NSA, die VIPS angehören, die Professionalität der unabhängigen forensischen Untersuchung bestätigt.

Die jüngsten forensischen Studien füllen eine entscheidende Lücke aus. Warum das FBI es versäumt hat, eine unabhängige kriminaltechnische Untersuchung des originalen „Guccifer 2.0"-Materials durchzuführen, bleibt ein Rätsel. – Ebenso rätselhaft bleibt, warum die „handverlesenen Analysten" des FBI, der CIA und der NSA, die den Geheimdienstbericht vom 6. Januar verfasst haben, einer kriminaltechnischen Untersuchung keinerlei Beachtung schenkten.

ANMERKUNG: Im Zusammenhang mit Hackerangriffen gibt es eine große Vermischung der Vorwürfe, weshalb wir klarstellen wollen, was der primäre Fokus unseres Memorandums ist. Wir konzentrieren uns insbesondere auf den angeblichen „Guccifer 2.0-Hack" vom 5. Juli 2016 auf den DNC-Server. In früheren VIPS-Memoranden wiesen wir auf die fehlenden Beweise für eine Verbindung zwischen dem angeblichen Guccifer 2.0-Hackerangriff und WikiLeaks hin. Und wir baten Präsident Obama ganz konkret, jedwede Beweismittel darüber offenzulegen, dass WikiLeaks die DNC-Daten von den Russen erhalten hat. [s. https://consortiumnews.com/2017/01/17/a-demand-for-russian-hacking-proof/ und https://consortiumnews.com/2016/12/12/us-intel-vets-dispute-russia-hacking-claims/]

Als Obama während seiner letzten Pressekonferenz im Amt des Präsidenten (18. Januar) diesen Punkt ansprach, bezeichnete er die „Schlussfolgerungen der Geheimdienste" als „nicht schlüssig", obwohl die Dienste in ihrem Bericht vom 6. Januar ihr „großes Vertrauen" („high confidence") in die These zum Ausdruck brachten, laut der russischen Geheimdienste „das DNC-Material, das sie sich angeeignet hatten, an WikiLeaks weitergaben".

Obamas Einlassung hat uns nicht überrascht. Es ist uns schon lange klar, dass der Grund, warum die US-Regierung keine schlüssigen Beweise für eine Weitergabe eines „russischen Hacks" an WikiLeaks hat, darin zu finden ist, dass es einen solchen Transfer nicht gab. Basierend auf der einzigartigen technischen Erfahrung unserer Ex-NSA-Kollegen sagen wir seit fast einem Jahr, dass die DNC-Daten durch eine Kopie beziehungsweise einen Leak eines DNC-Mitarbeiters an WikiLeaks gelangten (bei dem es sich aber mit nahezu Sicherheit nicht um dieselbe Person handelt, die die DNC-Daten am 5. Juli 2016 kopiert hat).

Aus den verfügbaren Informationen schließen wir, dass ein und derselbe interne DNC-Kopier-/Leak-Prozess zu zwei verschiedenen Zeitpunkten von zwei unterschiedlichen Entitäten für zwei deutlich unterscheidbare Zwecke verwendet wurde:

(1) ein Leak eines Insiders an WikiLeaks noch bevor Julian Assange am 12. Juni 2016 angekündigt hatte, dass er im Besitz von DNC-Dokumente sei, die er zu veröffentlichen beabsichtige (was er am 22. Juli auch tat) – die vermutliche Absicht hinter dem Leak war, die große Voreingenommenheit der Parteiführung der Demokraten zugunsten der Kandidatin Hillary Clinton; und

(2) ein separater Leak vom 5. Juli 2016, der vorbeugend die späteren WikiLeaks-Veröffentlichungen diskreditieren sollte, indem er „aufzeigte", dass diese auf einem „russischen Hackerangriff" basieren.

Herr Präsident:

Dies ist unser erstes Memorandum als Veteran Intelligence Professionals for Sanity (VIPS) an Sie. In der Vergangenheit haben wir es US-Präsidenten wissen lassen, wenn wir der Ansicht waren, dass unsere Geheimdienstkollegen einen wichtigen Sachverhalt falsch erfasst haben und warum. Zum Beispiel warnte unser erstes Memorandum [s. https://consortiumnews.com/2003/02/05/powells-un-speech-and-the-case-for-war/], das sich auf Außenminister Colin Powells UN-Rede am 5. Februar 2003 bezog und noch am selben Tag an Präsident George W. Bush herausging, dass die „unbeabsichtigten Konsequenzen wahrscheinlich katastrophal sein würden", sollten die USA den Irak angreifen und diesen Krieg auf Geheimdienstinformationen begründen, die wir Geheimdienstveteranen sogleich als falsch erkannt hatten und die von einer Kriegsagenda bestimmt waren.

Die „Einschätzung der Geheimdienstgemeinschaft" vom 6. Januar 2017 [s. unter https://en.wikipedia.org/wiki/File:Intelligence_Community_Assessment_-_Assessing_Russian_Activities_and_Intentions_in_Recent_US_Elections.pdf], die von „handverlesenen" Analysten des FBI, der CIA und der NSA erstellt wurde, scheint ebenso auf einer Agenda zu beruhen. Dieser Bericht fußt weitestgehend auf der „Einschätzung", – die von keinerlei ersichtlichen Beweisen gestützt wird – dass eine schattenhafte Organisation mit dem Spitznamen „Guccifer 2.0" im Auftrag des russischen Geheimdiensts in die Rechner des Nationalen Komitees der Demokraten (DNC) eingedrungen war und die dabei entwendeten E-Mails an WikiLeaks weitergegeben hat.

Die oben erwähnten jüngsten forensischen Befunde lassen diese Einschätzung unglaubwürdig erscheinen und wecken starke Zweifel an den Grundlagen der außergewöhnlich erfolgreichen Kampagne, die Russlands Regierung der Hackerangriffe bezichtigt.

Die Experten und Politiker, die lautstark Anklage gegen die russische „Einmischung" in die US-Wahlen erheben, werden erwartungsgemäß die forensischen Erkenntnisse in Zweifel ziehen, falls diese jemals von den Mainstream-Medien aufgegriffen werden. Aber physikalische Prinzipien lügen nicht; und die technischen Einschränkungen des heutigen Internets werden weithin verstanden. Wir sind bereit, uns allen stichhaltigen Einwänden gegenüber den Erkenntnissen der forensischen Untersuchungen zu stellen.

Vielleicht möchten Sie CIA-Direktor Mike Pompeo fragen, was er darüber weiß. Unsere eigenen, langjährigen Erfahrungen in der Geheimdienstgemeinschaft deuten darauf hin, dass es möglich ist, dass weder der ehemalige CIA-Direktor John Brennan noch die Cyber-Krieger, die für ihn arbeiteten, völlig aufrichtig gegenüber ihrem neuen Direktor waren, was den ganzen Ablauf der Angelegenheit betrifft.

Kopiert, nicht gehackt

Wie oben angedeutet, konzentrierte sich die gerade erst abgeschlossene unabhängige forensische Arbeit auf Daten, die von einer geheimnisvollen Person namens „Guccifer 2.0" kopiert wurden (nicht gehackt). Die Forensik spiegelt die offenbar verzweifelte Anstrengung wider, „den Russen" die Schuld für die Veröffentlichung der verfänglichen DNC-E-Mails – drei Tage vor dem Parteitag der Demokraten im Juli 2016 – zuzuschieben.

Da die E-Mails auf eine starke Voreingenommenheit zugunsten Clintons schließen ließ, war ihr Wahlkampfteam bestrebt, von deren Inhalt auf deren Herkunft abzulenken – also die Frage, wer „hackte" diese E-Mails? Diese Kampagne wurde enthusiastisch von willfährigen Mainstream-Medien unterstützt.

„Die Russen“ waren der ideale Schuldige. Und nachdem WikiLeaks-Gründer Julian Assange am 12. Juni 2016 ankündigte: „Wir haben E-Mails zu Hillary Clinton, die auf ihre Veröffentlichung warten“, hatte Clintons Team über einen Monat Zeit, um vor dem Parteitag seine eigenen „forensischen Fakten“ anzubringen und die Medien dazu zu bewegen, sich auf die „russische Einmischung“ einzuschießen.

Clintons PR-Chefin Jennifer Palmieri hat erklärt, wie sie auf dem Parteitag ein Golfmobil nutzte, um alle Medienvertreter erreichen zu können. Sie schrieb, dass es ihre „Mission war, die Aufmerksamkeit der Presse auf etwas zu richten, das selbst von uns nur schwer zu verarbeiten war: Die Aussicht, dass Russland nicht nur E-Mails vom DNC-Server gehackt und gestohlen hat, sondern dies in der Absicht tat, Donald Trump zu helfen und Hillary Clinton zu schaden.“ [Ihr Artikel ist nachzulesen unter https://www.washingtonpost.com/posteverything/wp/2017/03/24/the-clinton-campaign-warned-you-about-russia-but-nobody-listened-to-us/?utm_term=.57c01b9e05d2 .]

Unabhängige Cyber-Ermittler haben nun die Art der forensischen Arbeit abgeschlossen, die die US-Geheimdienste in ihrer Einschätzung vom 6. Januar unterlassen haben. Seltsamerweise begnügten sich die „handverlesenen“ Geheimdienstanalysten damit, dieses und jenes „einzuschätzen“ und „abzuwägen“. Im Gegensatz dazu gingen die Ermittler der Sache auf den Grund und kamen mit überprüfbaren Beweisen zurück, die sie in den Metadaten der Aufzeichnungen des angeblichen russischen Hackerangriffs gefunden hatten.

Sie fanden heraus, dass der vermeintliche DNC-Hack von Guccifer 2.0 gar kein Hack war, weder von Russland noch jemanden anders. Vielmehr entstammt er einer Kopie (auf ein externes Speichergerät – zum Beispiel einem USB-Stick), die von einem Insider angefertigt wurde.

Die Daten wurden geleakt, nachdem sie per Cut-and-Paste manipuliert worden waren, um den Verdacht auf Russland zu lenken. Wir wissen nicht, bei wem oder was es sich um den undurchsichtigen Gufficer 2.0 handelt. Vielleicht möchten Sie dazu das FBI befragen.

Die zeitliche Abfolge

12. Juni 2016: Assange kündigt die Veröffentlichung von E-Mails über Hillary Clinton an. [s. https://wikileaks.org/dnc-emails/]

15. Juni 2016: Die vom DNC beauftragte IT-Firma Crowdstrike (die einen fragwürdigen Hintergrund hat und sich in einem Interessenkonflikt befindet [weitere Infos dazu unter https://deutsch.rt.com/nordamerika/50642-schlechte-verliererin-clinton-beschloss-sofort-moskau-schuld-geben/]), verkündet, Belege dafür zu haben, dass auf dem DNC-Server eine Schadsoftware gefunden wurde, die dort von Russen platziert wurde.

15. Juni 2016: Am selben Tag bestätigt „Gufficer 2.0“ die Aussage und übernimmt die Verantwortung für den „Hack“; behauptet, eine WikiLeaks-Quelle zu sein; und veröffentlicht ein Dokument, das, wie eine forensische Untersuchung ergab, voller künstlich eingefügter „russischer Fingerabdrücke“ ist.

Wir glauben nicht, dass es sich bei der Abfolge zwischen dem 12. und 15. Juni um einen Zufall handelt. Vielmehr spricht diese für einen präventiven Schachzug, bei dem Russland in Verbindung mit allem gebracht werden sollte, was WikiLeaks veröffentlichen würde, und der zeigen sollte, dass alles auf einen russischen Hackerangriff beruht.

Das Schlüsselereignis

5. Juli 2016: Am frühen Abend (Eastern Daylight Time (EDT) / Sommerzeit Ostküste) hat

jemand, der in der EDT-Zeitzone arbeitet, mit einem Computer, der direkt mit dem DNC-Server oder dem lokalen DNC-Netzwerk verbunden war, 1,976 Gigabyte Daten in 87 Sekunden auf ein externes Speichergerät kopiert. Diese Geschwindigkeit ist um ein Vielfaches höher, als es mit einem Hack physikalisch möglich wäre.

Es scheint daher, dass es sich bei dem von der selbsternannten WikiLeaks-Quelle Gufficer 2.0 behaupteten DNC-Hack nicht um einen Hack von Russland oder irgendjemand anderen handelte. Stattdessen handelte es sich um eine Kopie von DNC-Daten auf ein externes Speichermedium.

Darüber hinaus förderte die kriminaltechnische Untersuchung der Metadaten zu Tage, dass im Nachhinein künstlich Daten per Cut-and-Paste anhand einer russischen Vorlage („template“) hinzugefügt wurden, mit dem klaren Ziel, die Daten einem „russischen Hack“ zuordnen zu können. Das alles spielte sich innerhalb der Zeitzone der Ostküste ab.

„Verschleierung und Rück-Verschleierung“

Herr Präsident, die weiter unten beschriebene Enthüllung kann damit in einem Zusammenhang stehen. Und selbst wenn das nicht der Fall sein sollte, denken wir, dass wir Sie darauf aufmerksam machen sollten. Am 7. März 2017 hat WikiLeaks damit begonnen, einen Fundus originaler CIA-Dokumente unter der Bezeichnung „Vault 7“ zu veröffentlichen. Nach eigener Aussage hat WikiLeaks die Dokumente von einem ehemaligen Auftragnehmer der CIA erhalten. Die Plattform beschreibt sie als in ihrem Ausmaß und ihrer Bedeutung vergleichbar mit den Informationen, die Edward Snowden im Jahr 2013 an Journalisten weitergab.

Niemand hat die Echtheit der Vault 7-Originaldokumente angezweifelt, die eine breite Palette von Werkzeugen zur Cyber-Kriegsführung offenlegten, die – wahrscheinlich mit der Hilfe der NSA – von der CIA-Abteilung für Digitale Innovation entwickelt wurden, die im Jahr 2015 von John Brennan ins Leben gerufen wurde.

Über diese kaum vorstellbaren digitalen Werkzeuge - die die Kontrolle über Ihr Auto übernehmen und es zum Beispiel auf über 100 Meilen pro Stunde beschleunigen können oder die die Fernspionage durch einen Fernseher ermöglichen – hatten die New York Times und andere Medien im Laufe des Monats März gebührend berichtet. Aber der dritte Teil der Vault 7-Veröffentlichungen, bei dem am 31. März das „Marble Framework“-Programm enthüllt wurde, wurde offenbar als zu heikel betrachtet, um Eingang in die Berichterstattung der New York Times zu finden.

Doch Ellen Nakashima von der Washington Post übte sich nicht in Verschwiegenheit. Ihr Artikel vom 31. März trug den packenden (und zutreffenden) Titel:

> WikiLeaks jüngste Veröffentlichung von CIA-Cyberwerkzeugen könnte die Hackeroperationen der Behörde auffliegen lassen. [s. https://www.washingtonpost.com/world/national-security/wikileaks-latest-release-of-cia-cyber-tools-could-blow-the-cover-on-agency-hacking-operations/2017/03/31/63fc3616-1636-11e7-833c-503e1f6394c9_story.html?utm_term=.c728b2991be8]

Die WikiLeaks-Veröffentlichung deutet daraufhin, dass „Marble“ für eine flexible und einfach zu bedienende „Verschleierung“ entworfen wurde und dass der Quellcode des Programms einen „Rück-Verschleierer“ („Deobfuscator“) enthält, um die Verschleierung der CIA rückgängig machen zu können.

Noch wichtiger ist, dass die CIA Berichten zufolge „Marble“ während des Jahres 2016 verwendet hat. Diesen Punkt ließ Nakashima in ihrem Artikel aus. Sie wies aber auf einen anderen wesentlichen Aspekt hin, auf den WikiLeaks aufmerksam gemacht hatte, nämlich, dass das Verschleierungswerkzeug ein „doppeltes Spiel bei der kriminaltechnischen Zuordnung“ erlaubt, beziehungsweise eine Operation unter falscher Flagge ist. Denn es enthält Sprachmuster in Chinesisch, Russisch, Koreanisch, Arabisch und Farsi.

Die Reaktion der CIA war gereizt. Deren Direktor Mike Pompeo nannte zwei Wochen später Assange und seine Mitarbeiter „Dämonen“ und wies daraufhin:

> Es ist Zeit, WikiLeaks als das zu bezeichnen, was es wirklich ist, ein nicht-staatlicher feindlicher Geheimdienst, der oft von staatlichen Akteuren wie Russland angetrieben wird." [s. http://thehill.com/policy/cybersecurity/328730-cia-director-wikileaks-a-non-state-hostile-intelligence-service]

Herr Präsident, wir wissen nicht, ob „Marble Framework“ oder Werkzeuge dieser Art eine Rolle bei der Kampagne spielten, die Russland des DNC-Hacks bezichtigt. Wir wissen auch nicht, wie ehrlich es die Mitarbeiter der CIA-Abteilung für Digitale Innovationen mit Ihnen und Direktor Pompeo meinen.

Putin und die Technologie

Wir wissen auch nicht, ob Sie Cyber-Themen im Detail mit Russlands Präsidenten Wladimir Putin besprochen haben. In seinem Interview mit Megyn Kelly von NBC schien er bereitwillig – vielleicht sogar erpicht darauf – zu sein, zu den Problemen im Zusammenhang mit Cyber-Werkzeugen Stellung zu nehmen, wie sie in dem Vault 7-Leak enthüllt wurden.

Putin wies darauf hin, dass die heutige Technologie es den Hackern ermöglicht, „maskiert und getarnt vorzugehen, sodass niemand den wahren Ursprung des Hackerangriffs ergründen kann. Und umgekehrt ist es möglich, es so zu arrangieren, dass jeder denkt, eine bestimmte Organisation oder Person sei die genaue Quelle der Attacke.“ „Hacker können überall sein“, sagte er.

„Vielleicht gibt es Hacker, auch in den Vereinigten Staaten, die mit cleveren und professionellen Methoden die Sache Russland unterschieben können. Können Sie sich ein solches Szenario vorstellen? Ich kann es …“

Vollständige Offenlegung:

In den letzten Jahrzehnten ist der Ethos unseres Geheimdienstberufes in der öffentlichen Wahrnehmung erodiert. Bis hin zu dem Punkt, an dem niemand mehr glaubt, dass es möglich ist, eine Analyse durchzuführen, die nicht von einer Agenda getrieben ist.

Daher möchten wir an dieser Stelle folgendes betonen: Wir von VIPS verfolgen keine politische Agenda; unser alleiniges Anliegen ist es, die Wahrheit zu verbreiten und, wenn nötig, unsere ehemaligen Geheimdienstkollegen zur Rechenschaft zu ziehen.

Wir sprechen und schreiben ohne Angst oder Gunst. Folglich ist jede Ähnlichkeit zwischen dem, was wir zu sagen haben, und dem, was Präsidenten, Politiker und Experten sagen, rein zufällig. Dass wir diese Tatsache ansprechen müssen, spricht Bände über diese hochpolitisierten Zeiten. Dies ist unser 50. VIPS-Memorandum seit der Rede von Colin Powell vor der UN. Unsere 49 vorher veröffentlichten Memos finden Sie unter https://consortiumnews.com/vips-memos/ .

Die Unterzeichner:

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)
Larry C Johnson, CIA & State Department (ret.)

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

(Damit ist endgültig geklärt, dass es sich bei der Behauptung, "russische Hacker hätten die Präsidentenwahl zugunsten Donald Trumps manipuliert", um eine von den US-Demokraten verbreitete Propagandalüge handelt. Anschließend drucken wir den Originaltext ab.)

Intel Vets Challenge 'Russia Hack' Evidence

In a memo to President Trump, a group of former U.S. intelligence officers, including NSA specialists, cite new forensic studies to challenge the claim of the key Jan. 6 "assessment" that Russia "hacked" Democratic emails last year.

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, 2016, 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 [see here and here].

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 Wiki-

Leaks, and we asked President Obama specifically to disclose any evidence that WikiLeaks received DNC data from the Russians [see here and here].

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 February 5, 2003, warned that the "unintended consequences were likely to be catastrophic," should the U.S. attack Iraq and "justfy" 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 Net-

work, 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 "deobfuscator" 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

(Signatures see end of translation.)

www.luftpost-kl.de
VISDP: Wolfgang Jung, Assenmacherstr. 28, 67659 Kaiserslautern