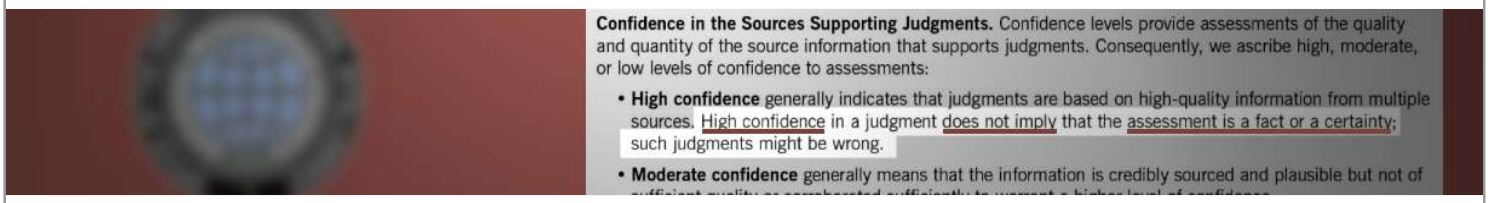

Non-Existent Foundation for Russian Hacking Charge

The findings and conclusions of this report are not intended to be pejorative, to malign any party, organization, or individual, particularly, our intelligence agencies, of which I have the highest respect. Herein are simply presentations of discovered facts which challenge the accepted theme of Russia being accused of interfering in the 2016 elections. A significant error has been perpetrated over time based on a flawed foundation of assumptions, which has resulted in excluding other possibilities.

Below is a summary of significant problems discovered with both the Dec. 29, 2016 Grizzly Steppe report and the January 06, 2017 Intelligence Community Assessment (ICA). Not all cyber intrusion tools, facilities, tactics, techniques, or procedures are exclusive to any one State or non-State player. The lack of exclusivity of the technical parameters and lack of traces simply cannot support a definitive conclusion as to source. Included also are extensive cyber-forensic investigations into the purported July 05, 2016 alleged Russian intrusion of DNC material by a Guccifer 2.0 persona and a material discovery within the alleged intrusion of June 15, 2016.

FINDINGS

1) The ICA and GRIZZLY STEPPE Reports lack disclosures and the ICA violated assessment requirements

2) Grizzly Steppe's Russia Foundation elements, "technical indicators", e.g., malware programs, IP addresses, and historical targets aren't unique to Russia and cannot be used to identify Russia or any other source

3) Trace routing of Fancy or Cozy Bear to Russia is non-existent

4) No link has been discovered to relate Wikileaks to Russia

5) Potential conflicts of Interest

6) Three previous Russian accusations strongly refuted

7) Forensic cyber analysis finds July 05 2016 intrusion was local download

8) Forensic cyber analysis finds June 15, 2016 intrusion had Russian fingerprints inserted.

9) Event timing from June 12, 2016 thru June 15, 2016 is highly suspicious

10) Non-State Players of significant means and motive have been ignored

ICA REPORT

In that there is not a single statement of proof in the entire report, the following disclaimers from page 13, widely ignored, should have been up front on page 01.

"Judgments are not intended to imply that we have proof that shows something to be a fact. ... Assessments are based on collected information, which is often incomplete or fragmentary, as well as logic, argumentation, and precedents."

Relevant here: It was reported in some stories that the Latvian Security Service fed CIA Director Brennan the assertion that the former had someone close to Putin. That's a foreign security service with its own anti-Russian axe. The degree to which the alleged Latvian report fed into the ICA is not known. It may possibly explain the NSA's "moderate" (approx. 50%) rather than "high" confidence in the ICA finding "We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances ... by discrediting... Clinton and publicly contrasting her... unfavorably to him."

(Sources 22, 31) Related: First paragraph of "ATLANTIC COUNCIL and CROWDSTRIKE FUNDING ..." below: Latvia (coincidentally?) is also one of the Atlantic Council's anti-Russian supporters. Further, also listed as Atlantic Council supporter, Ukrainian oligarch Victor Pinchuk, major contributor to Clinton Foundation, including when Mrs. Clinton was secretary of state, from the Victor Pinchuk Foundation, ..." This paragraph links both Latvia and Clinton back to preceding paragraph and NSA's not agreeing to "high" confidence.

Unfortunately, this report really is an embarrassment to intelligence professionalism. The ICA comes across as a series of assertions, free of relevant substance. It also fails to include key disclosures. In addition, it relies upon alleged Russian historical 'nature,' what this or that person said once, etc. Further, It failed to follow ODNI mandated assessment procedures, and did not include full participation of any of the named agencies.

MISSING ICA AND / OR GRIZZLY STEPPE DISCLOSURES:

These five relevant disclosures were not included in one or the other above reports.

1. The FBI, having asked multiple times at different levels, was refused access to the DNC server(s). It is not apparent that any law enforcement agency had access. *

2. The apparent single source of information on the purported DNC intrusion(s) was from Crowdstrike.

3. Crowdstrike is a cyber security firm hired by the Democratic Party.

4. Not the FBI, CIA, nor NSA organizations analyzed the information from Crowdstrike. Only picked analysts of these agencies were chosen to see this data and write the ICA.

5. The ICA is not an IC-Coordinated Assessment

* This non-disclosure statement (1 above) is based on Comey's testimony before the Senate Intelligence Committee on June 08, 2017. On July 05, 2017 a Crowdstrike statement appeared: "In May 2016 CrowdStrike was brought [in] to investigate ... under their direction we fully cooperated with every U.S. government request ... cooperation included ... providing of the forensic images of the DNC systems to the FBI." The question is whether these disk images were taken prior to or after the 'intrusions' in question. (Sources 26,27,28)

Adam Carter: "So, the most likely explanation, ... the FBI do not have disk images from any point during or following the alleged email hack. ... CrowdStrike's failure to produce evidence. – With Falcon installed between April and May (early May), they should have had evidence on when files/emails/etc were copied or sent. – That information has never been disclosed." Hence, No. 1 above stands. (Source 26)

MISSING LINK BETWEEN WIKILEAKS AND RUSSIA

Nowhere in the ICA was there any evidence of any connection between Russia and Wikileaks. Nor was there any demonstrated connection between Guccifer 2.0 and Wikileaks. There appeared to be an effort to show such a connections, but nothing of substance, other than conjecture was used to support the allegation. Concluding that such a connections exists is, frankly, dishonest and raises the question of motive to do such.

William Binney, previous Technical Director NSA: (Source 10)

"I've seen absolutely nothing that shows any involvement of the Russian government in passing data to WikiLeaks. ... It didn't prove anything to me. ... It didn't give the IP addresses, the Mac numbers or any other details about them. ... It also didn't show how they hacked in, and how they ex-filtrated the data, how much data they took. ... They didn't show any of that trace routing. And that's what they should have shown to prove it."

Assange on Leak Source (Source 25)

Assange of Wikileaks, the one who actually knows his sources, has been adamant all along that the Russian government was not a source; it was a non-state player. It could have been a Russian or any other non-state source. Assange, whatever one thinks of his releasing information, deals in truth; that's

what he does, and that's exactly why some hate him so. But Assange knows his sources, and unless our politicians, main media, and some analysts are omniscient, or unless they have actual evidence to the contrary, which they apparently do not, they have no honest business claiming otherwise, and such is dishonorable..

ASSANGE: Our source is not a state party

HANNITY: Can you say to the American people unequivocally that you did not get this information about the DNC, John Podesta's emails — can you tell the American people 1,000 percent you did not get it from Russia...

ASSANGE: Yes.

HANNITY: ... or anybody associated with Russia?

ASSANGE: We — we can say and we have said repeatedly... over the last two months, that our source is not the Russian government and it is not a state party.

Rep. Dana Rohrabacher met with Assange on Aug. 15, 2017. (Source 34)

Assange again stated no Russian involvement. Rohrabacher claimed: "Julian also indicated that he is open to further discussions regarding specific information about the DNC email incident that is currently unknown to the public." "We left with the understanding that we would be going into further details in the near future. The rest of the message is for the president directly and I hope to convey it to him as more details come in."

LACK OF GRIZZLY STEPPE FOUNDATIONS

The crux of this section is to demonstrate that none of the "technical indicators, e.g., cyber intrusion tools, facilities, tactics, techniques, or procedures or elements of the foundation upon which Russia is singled out as the perpetrator is unique to Russia and cannot be uniquely attributed to Russia as opposed to any other source. Sub-sets of these technical parameters are frequently found together, supporting the conclusion of an identifiable source, given a name, e.g., APT 28 or 29. However, it is pure assumption and, therefore, misleading to then conclude the pseudo-named source is Russia or any other sophisticated source without any trace proof back to a real source.

As an example, in Grizzly Steppe, page 2, second paragraph, beginning with, "Both groups have historically targeted ...," is there anything in that paragraph which can be claimed as unique to Russia or which excludes all other major state players in the world or any of the non-state organizations covered in NON-STATE PLAYERS of this report?

It is no secret that NSA has the technology to trace a web event, e.g., a cyber attack, back to its source. There has been no public claim, nor is it implied in either Grizzly Steppe or the ICA that the NSA has trace routing to Russia on any of these purported Russian hacks.

(APT = Advanced Persistent Threat) APT28, aka Fancy Bear, Sofacy, Strontium and APT29, aka Cozy Bear, CozyDuke are used as 'proof' of Russia 'hacking' by Russian Intelligence agencies GRU and FSB respectively. These conclusions are being accepted without any question by not only our Main Media, but apparently by some members of our intelligence community. Let's take a look at some interesting observations:

1) June 15, 2016 Dmitri Aperovitch, quoted in Atlantic Council article: (Source 9)

Q: "What evidence is there that these actors [Fancy Bear (GRU) and Cozy Bear (FSB)] are connected to the FSB or GRU?"

DA: "medium-level of confidence that FancyBear is GRU". "low-level of confidence that CozyBear is FSB,"

Above translates to an average level of confidence of approx. 37-38 %

This approx. 37-38% Level of Confidence is the basis for 'knowing' that Russia interfered, etc. To the public, it's only called "high level of confidence."

2) Despite such as above, it is taken for granted that Fancy Bear and Cozy Bear are GRU and FSB. Fancy and Cozy are sets of capabilities, attack tools and network infrastructure that are

widely assumed to automatically mean GRU and / or FSB, i.e., Russia.

The problem is that apparently not a single element of either have actually ever been traced back to Russia, i.e., no trace routing, let alone to GRU or FSB. The 'certainty' is based upon conjecture upon conjecture, e.g., 'who else could it be'? One historical excuse given is some of the type files accessed, as if only Russia could have an interest. Such reasoning is shallow at best. There are actually some very serious, highly financed, well organized other state and non-state players with substantial motives. The lack of even considering such is suspicious, and evidence of a lack of real investigation.

ESET (A cyber security firm with offices world-wide): "As security researchers, what we call "the Sednit group" [Another acronym for Fancy Bear, APT28, etc.,] is merely a set of software and the related network infrastructure, which we can hardly correlate with any specific organization." (Source 13)

3) "Indicators" provided by DHS were used to identify 'Russian' attack program and IP addresses. (Sources 7 and 8)

The program, attributed to a "Grizzly Steppe", identified (by reverse engineering) is identified as Ukrainian P.A.S. 3.1.0. This program is an off-the shelf tool available to anyone. Further, this was an old version (most recent having been 4.1.0.). Highly unlikely that the GRU would use an old level off the shelf tool. And, not to pass over the point too rapidly, this program is Ukrainian, not Russian.

"DHS provided 876 IP addresses as part of the package of indicators of compromise, globally distributed ... they originate from 61 countries and 389 different organizations with no clear attribution to Russia ...

they don't appear to provide any association with Russia."

4) Gregory Copley, President, International Strategic Studies Association (ISSA), Editor-in-Chief of Defense & Foreign Affairs, and the Global Information System (GIS): (Source 11)

"This is a highly politically motivated and a subjective report which was issued by the intelligence community. ... does not present evidence of successful or even an attempt to actually actively manipulate the election process. .... This intelligence report and all of the claims about this so called hacking is an attempt to shoot the messenger rather than to allow the people to focus on the message. ...".

5) Jeffrey Carr: Principal consultant 20KLeague.com, Founder of Suits and Spooks; Author of "Inside Cyber Warfare," lecturer at the Army War College and the Defense Intelligence Agency.: (Source 12)

"The X-Agent malware is not exclusive to Russia. ... acquired by at least one Ukrainian hacker group and one European cybersecurity company, ... means that others have it as well. "Exclusive use" is a myth ... attacks attributed to the GRU were a comedy of errors; not the actions of a sophisticated adversary. ... Crowdstrike's Danger Close report, [on purported hack of Ukrainian Howitzers] ... supposed to be the nail in the coffin ... that proved the GRU .... DNC hack, ... repudiated by the Ukrainian government, the IISS whose data they misused ... [and] the builder of the military app that they claimed was compromised...."

6) Jeffrey Carr: (As above). (Source 13)

"... "the Sednit group" [another synonym for Fancy Bear, APT28, etc.] is merely a set of software and the related network infrastructure, ... we can hardly correlate with any specific organization. ESET doesn't assign APT28/Fancy Bear/Sednit to a Russian Intelligence Service or anyone else for a very simple reason. Once malware is deployed, it is no longer under the control of the hacker who deployed it or the developer who created it. It can be reverse-engineered, copied, modified, shared and redeployed does not assign to Russian Intelligence or anyone else."

ESET: "As security researchers, what we call "the Sednit group" is merely a set of software and the related network infrastructure, which we can hardly correlate with any specific organization."

"... X-Agent, used in the DNC, Bundestag, and TV5Monde attacks. ... foolish and baseless to claim, as Crowdstrike does, that X-Agent is used solely by the Russian government when the source code is there for anyone to find and use at will."

7) The Claim that Guccifer2.0 Used a Private Russian VPN (Source 1)

It has been alleged that Guccifer 2.0 used a private Russian VPN of Elite-VPN.

Adam Carter (Source 1) contacted the provider of Elite-VPN, and found out that the supposed "exclusive" IP address was NEVER exclusive. Within the source identified above, one will find the communications between Adam Carter and the owner of Elite-VPN.

An excerpt from the owner's reply back to Adam: "... the IP address referred to in the article is not "private." It is a public IP address and it is accessible to any internet user. The only reason why it is not listed is because it is the 'default' address for this server, that is, it does not need to be selected, this address is provided right after the connection." The owner of the VPN service was very concerned and upset of the inference that his server was being accused as providing a private Russian link.

Bottom line: The alleged "private" Russian link was neither private nor Russian.

IC-COORDINATED ASSESSMENT

What is an "IC-Coordinated Assessment?" It is a formal, mandated "Intelligence Community" coordinated assessment. Due to the Iraq WMD fiasco any IC assessment must include balance, such as a competitive analysis, or competing views or analysis of alternatives. In ODNI words it is mandated to include an "analysis of alternatives". This requirement of an IC assessment was ignored by the ICA process. Further, by hand-picking selected analysts from the agencies, bypassing normal agency procedures, apparently limiting the technical aspect of the investigation to that which Crowdstrike provided, yet using IC in the title, as if this were a full three agency participation, is a deception. There was no apparent full participation by any of the agencies, FBI, CIA, NSA.

ATLANTIC COUNCIL and CROWDSTRIKE FUNDING (Sources 22, 23)

Crowdstrike co-founder and Director of Technology, Dmitri Alperovitch, is also a nonresident senior fellow of the Atlantic Council. The question of potential Conflicts of Interest should be raised concerning Crowdstrike's link to the Atlantic Council when one notes the significant links to anti-Russian contributors to the Atlantic Council. The Atlantic Council itself can certainly not be considered neutral to Russia.

James Carden, The Nation, Jan. 03, 2017: (Source 22)

Alperovitch [is] "... head honcho of its "Cyber Statecraft Initiative" – of which his role in promoting the "Putin did it" scenario is a Exhibit A. ...

The connection between Alperovitch and the Atlantic Council has gone largely unremarked upon, but it is relevant given that the Atlantic Council – which is funded in part by the US State Department, NATO, the governments of Latvia and Lithuania, the Ukrainian World Congress, and the Ukrainian oligarch Victor Pinchuk – has been among the loudest voices calling for a new Cold War with Russia."

Adam Johnson, FAIR, June 16, 2016: (Source 23)

Other supporters of the Atlantic Council: "a consortium of Western corporations (Qualcomm, Coca-Cola, The Blackstone Group), including weapons manufacturers (Lockheed Martin, Raytheon, Northrop Grumman) and oil companies (ExxonMobil, Shell, Chevron, BP)."

PREVIOUS RUSSIAN ACCUSATIONS REFUTED

With high respect for the firm and executives of Crowdstrike, it does an outstanding job in finding and protecting against cyber attacks. Nevertheless, it appears that identification of the source may leave room for improvement, especially the apparent tendency to immediately allege that Russia is the perpetrator, perhaps sometimes better to recuse themselves.

Dmitri Aperovitch, chief technical officer of Crowdstrike, has voiced anti-Russian, opinions and is a Senior Fellow of the Atlantic Council, itself anti-Russian. That is hardly neutral. Crowdstrike also accused Russia of interfering in political affairs of France and Germany and hacking Ukrainian military howitzers to make them inoperable. All three claims have been refuted, ranging from lack of evidence to outright denial, the first two by the French and German intelligence, and the third as detailed below:

THE PURPORTED HACK of UKRAINIAN HOWITZERS BY GRU

The following summary of events are drawn from these sources, including the increased confidence level of Fancy Bear being GRU from Medium to High.

(Sources 13, 14, 15, 16, 17, 18, 19, 20, 21)

Dmitri Alperovitch claimed that Fancy Bear, using a variant of X-Agent, a program supposedly unique to Fancy Bear, had hacked the Ukrainian Kiev army's Howitzers, significantly reducing their readiness inventory in their war against the Donbass region. Because this purported hack would benefit Russia militarily, Alperovitch concluded that the GRU was responsible, and, therefore, evidence that Fancy Bear was the GRU.

Alperovitch, Crowdstrike, Dec 22, 2016: "From late 2014 and through 2016, FANCY BEAR X-Agent implant was covertly distributed on Ukrainian military forums within a legitimate Android application ... Ukrainian artillery forces have lost over 50% of their weapons in the two years of conflict and over 80% of D-30 howitzers, the highest percentage of loss of any other artillery pieces in Ukraine's arsenal."

Alperovitch, PBS News Hour, Dec 22, 2016: "Ukraine's artillery men were targeted by the same hackers, that we call Fancy Bear, that targeted DNC, but this time they were targeting cell phones to try to understand their location so that the Russian artillery forces can actually target them in the open battle. It was the same variant of the same malicious code that we had seen at the DNC."

Alperovitch then used this claimed successful hack by the GRU to claim it proved that the GRU had also hacked the DNC, as Fancy Bear had hacked both and was the GRU. Alperovitch therefore claimed, and the Washington Post made a headline story of it, that Crowdstrike was raising its confidence level of Fancy Bear being the GRU from middle to high confidence.

Problems: Alperovitch had misused a report by the International Institute for Strategic Studies (IISS), concerning a change in Army field howitzer inventory numbers. The reduction in inventory was reportedly due to a redeployment from field to the Airborne. None had been 'hacked' by GRU or anyone else nor removed from service. And this inventory transfer had occurred in 2013, prior to the Kiev Army – Donbass area war which began in 2014.

It has also been claimed that the Apple App, originally written by an artillery officer, when modified would not have worked as advertised due to GPS and distance limitations.

IISS not only complained of the mis-use of its report, but the alleged hack was refuted by field artillery officers, the Kiev army chain of command and the Kiev government as never having happened. No wonder, as the transfer of the Howitzers from one organization to another happened in 2013.

Additionally, X-Agent, allegedly used against the Ukrainians is not unique to anyone, and could not be used to claim use by the GRU no more than anyone else.

ESET (International Cyber Security firm) obtained the entire source code of X-Agent company. ESET: "During our investigations, we were able to retrieve the complete X-Agent source code for the Linux operating system...."

Jeffrey Carr: "If ESET could do it, so can others. It is both foolish and baseless to claim, as Crowdstrike does, that X-Agent is used solely by the Russian government when the source code is there for anyone to find and use at will."

The use of this alleged hack to up the confidence level of Fancy Bear being the GRU from Medium to High was without foundation. Crowdstrike should have reduced their confidence level back down from High to Medium, the latter quoted in the June 15, 2016 Aperovitch quote in Atlantic Council article (Source 9). Not aware of that correction having been made, and if not made, then a deception.

RUSSIAN LANGUAGE and/or a RUSSIAN NAME USED

If one does not have trace routing of an attack back to the source, one cannot assert with high confidence that it is from a given source. Conjecture, based on assumptions does not provide a basis for serious allegations, particularly when such can lead to the weakening of our government or even to war with a nuclear power.

Forensicator Observation: "... the NSA would have been in the best position to nail down attribution with high confidence. I'm sure they could have found some way to make those claims and convince the public they had information to back up the claims without disclosing sources and methods. They made no such definitive statements."

It is ridiculous to assert that because a hack used or that had been found within a hack either Russian language and/or any Russian name, no matter how famous, that it can be concluded that 'Russia did it.' Such is nonsense. A language can be used or a name can be inserted anywhere in the world. It is almost childish to blame any nation, because their language or a famous name is found within a claimed hack.

The following is not to imply that what is described was used on the DNC purported 'hacks'. It is an example of the level of evolving cyber attack sophistication. Wikileaks release Vault 7, March 31, 2017 (Source 24): The CIA had operational 'during 2016', with 1.0 available in 2015, a cyber-intrusion tool entitled Marble Framework. Marble is an anti-forensic, masking, obfuscation tool to "hamper forensic investigators and anti-virus companies from attributing viruses, trojans and hacking attacks to the CIA."

It is specifically designed to act as a false flag cyber attack tool, by using a target language, to make it look like Russia, China, Iran, etc. were the villains of a cyber attack.

As knowledge of Marble has long since been in the public domain, as well as the source code itself, it is disingenuous for both our main media and screaming Russiagate politicians not to acknowledge such and its implications.

HIGHLY COINCIDENTAL TIMING

The timing between Assange announcement of pending Hillary Clinton emails of June 12, 2016 and the June 14, 2016 (only two days) Crowdstrike Russian hacking announcement and the following day, June 15th , emergence of a Guccifer 2.0 persona alleging to be a Wikileaks source, strongly implies motive to taint anything coming from Wikileaks as Russian sourced. See "expanded explanations" (See "expanded explanations" (Source 1)

Additionally, on the June 15, 2016 alleged Russian 'hack' it was discovered that "Russian Fingerprints" were inserted beneath the Guccifer 2.0 persona layer; (using "cut and paste" into "Russian Stylesheet[s] that existed in multiple documents even before the content in each document did."). (See "expanded explanations" (Sources 2,3,4,29)

There has even been some speculation of the possibility that due to the level of technical expertise demonstrated by Guccifer 2.0 persona, the excellent English language articulation (no direct / indirect article errors) and U.S. Software development process knowledge of the Guccifer 2.0 speaker, in conjunction with the curious timing relationship between the June 14, 2016

Crowdstrike announcement and June 15th Guccifer 2.0 persona popping up, that one of the involved U.S. parties might have some involvement in the Guccifer 2.0 persona.

CYBER-FORENSIC INVESTIGATIONS:

Recent discoveries by independent cyber forensic experts at the meta-data level of the alleged Guccifer 2.0 cyber intrusion of the DNC records on July 05 2016, have raised serious questions of alleged Russian hacking.

On July 04 2016 and July 06 there were posts by the Guccifer 2.0 persona. They are about the July 05 purported 'hack' or download, the subject of the following technical analysis. (Sources 30,32)

July 4: "Happy #IndependenceDay!!! Wait for a new #dnchack release tomorrow"

July 6: "Trumpocalypse and other DNC plans for July ... I have a new bunch of docs from the DNC server for you. ... It includes the DNC action plan during the Republican National Convention, Surrogate Report, POTUS briefing, financial reports, etc. ... This pack was announced two days ago but I had to keep you waiting for some security reasons. I suffered two attacks on my wp account. ..."

To assist the reader in focusing on the relevant, and not tangential, here's the overall perspective and objectives of Forensicator on the analyzed July 05 2016 event:

" ... any conclusions reached from an analysis activity will be balance of hard facts and judgements based on experience and perceived probabilities and plausibilities. Note that the transfer speed argument comes in two parts: 1. it supports the local copy conclusion, and suggests a conclusion that a USB 2 media was the target. 2. It is used to reject the conclusion that such a transfer rate can be achieved when transmitting data from DC back to Romania. ... my main goal was to refute the "Guccifer 2 as a remote Romanian/Russian hacker" narrative. ... some people have moved the narrative to "local accomplice" ... theory hasn't got much traction perhaps because there is a fine line between a local accomplice and an insider serving as leaker."

The cyber-forensic sources listed below have done what the ICA hand-selected, sequestered analysts did not do. They went in depth and provided actual verifiable evidence from the meta-data records of the July 05 2016 alleged Guccifer 2.0 Russian intrusion of DNC records in support of conclusions.

CYBER-FORENSIC CONCLUSIONS:

Overall Summary: Based on available information pertaining to July 05. 2016, excellent cyber forensic in depth analysis, and probabilities and plausibilities, there was no July 05 2016 Guccifer 2.0 Russian "hack." It was a purposeful leak downloaded on the US East Coast by someone with direct access or via LAN to the DNC server or copy of its data onto external storage, e.g., 2.0 thumb drive. Incidentally, metadata analysts on the June 15 2016 alleged Russian 'hack', otherwise not a subject of this report, discovered that Russian fingerprints had been deliberately inserted under the Guccifer 2.0 label, with the apparent objective of discrediting Wikileaks and any following leaks or whistleblowers. This latter subject is covered in more depths near the end of this report.

Forensicator (Sources 3 and 5):

The purported July 05 2016 "hack" by Guccifer 2.0 of DNC was a purposeful "leak."

Forensic analysis discovered three findings significant to the conclusion:

Transfer rate of data relative to internet mid-2016

Rate matching actual, not advertised, USB 2.0 transfer rate

All times East Coast

The alleged "hack" was effectively impossible in mid-2016. The required download speed of the "hack" precludes an internet transfer of any significant distance, even at today's (2017) rates. On July 05 2016, 1,976 MegaBytes were transferred in 87 seconds. That comes to approx. 23 MB/s (bytes, not bits).

EAST COAST July 2016

(keep in mind, we are talking a year ago, not what is possible in 2017)

1) 1975.583 MegaBytes transferred

2) Elapsed time 87.353 seconds

3) Transfer rate 22.616 MB/s

"A transfer rate of 23 MB/s is estimated for this initial file collection operation. This transfer rate can be achieved when files are copied over a LAN, but this rate is too fast to support the hypothesis that the DNC data was initially copied over the Internet (esp. to Romania)."

Downloaded onto external storage, e.g., 2.0 thumb drive

Downloaded using computer directly connected or via LAN to DNC data

Transfer speed of 22.6 MB/s matches speed of 2.0 thumb drive after overhead

Occurred somewhere within the US Eastern time zone on July 05 2016

"Timezone remained set as Eastern time throughout all dates of transfers and while system clocks and locale settings can, of course, be changed – it would be illogical for someone claiming to be in Romania – to set their timezone to something that would then contradict it."

Forensicator August 03 2017 test update: (See source 5)

The Forensicator conducted further extensive tests to re-affirm previous conclusions.

" ... that transfer rates of 23 MB/s (Mega Bytes per second) are not just highly unlikely, but effectively impossible to accomplish when communicating over the Internet at any significant distance. Further, local copy speeds are measured, demonstrating that 23 MB/s is a typical transfer rate when writing a USB-2 flash device (thumb drive). ... In practice, actual transmission rates will fall well below the theoretical rates, ... packets transmitted over the Internet have to transit many switches and must share bandwidth ... copying multiple small files will increase the need for "hand-shaking" ... further decreases the effective transmission speed. ... distance traveled can have a major impact ... accessing a host on the opposite coast cut the download speed by a factor of 7. ... drop into the range of 1 MB/s to 2 MB/s when communicating through Romanian, Ukrainian, or Russian VPN servers."

"In conclusion the performance data above strongly supports the original statement in the study: "A transfer rate of 23 MB/s is estimated for this initial file collection operation. This transfer rate can be achieved when files are copied over a LAN, but this rate is too fast to support the hypothesis that the DNC data was initially copied over the Internet (esp. to Romania)."

Adam Carter (Source 1) on Forensicator: "Forensicator's ability to aggregate data, extrapolate datasets and produce further information on which new conclusions can be formed (such as working out transfer

speeds, time zones used over time, timestamp resolution and the implications of each) was akin to someone having a key to unlock data that had previously been locked away due to apparent obscurity in isolation (The simplest example of this being that a single file timestamp tell us nothing about speeds of file transfers but an array of them, considered collectively, does)."

ISPS speed report of August 2016: speedtest.net – reports – united-states (See source 6 below)

US Fastest ISPS – Average speeds

Xfinity 125 Mb/s 15.6 MB/s

Cox 118 Mbs 14.7 MB/s

July 05 2016 transfer rate: 22.6 MB/s

"The largest contributions to this increase came in the month of June from XFINITY and Cox Communications with average download speeds of 132.08 Mbps [16.5 MB/s] and 162.14 Mbps, [20.25] respectively. The newly-created Spectrum ... ending the same period with a combined 131.97 Mbps [16.5 MB/s]."

There were reportedly some higher peak speeds recorded, but none known to have reached the 22.6 MB/s transfer rate. In July 2016 Google fiber was implemented in Atlanta, as first for East timezone, but not by July 05, and not in Washington DC.

Some issues raised to attempt to refute the above findings are convoluted stretches, with multiple increased dependencies for any hacker to risk. It is always imperative to minimize dependencies, and convoluted stretches are not the way to go.

Adam carter made an important observation: "Forensicator analyzed, made observations and gave the most probable explanations based on those observations. It is NOT incumbent on him to disprove convoluted and unsubstantiated theories people can imagine in order to demonstrate that his findings are the most probable." (Source 33)

Some author observations on hypotheticals, metadata, and the Falcon cyber protections system

First, metadata is simply data about other data; it is generally perspective information about data, e.g., time stamps, size, source, destination, etc. It'll vary depending on the subject. True, metadata can be altered. However, there should be a logical reason for doing so. There is little reason to believe that the 5th is not valid. Guccifer 2.0 himself bracketed it with his 4th and 6th posts, and nothing was found in the metadata analysis to invalidate the date itself, regardless of whether the activity was a hack or local copy. As for the time zone being altered, it would make no sense to change to the US Eastern zone when the objective is to prove it is Romanian or Russian.

These findings are not based on hypotheticals, but on the most probable logical conclusions derived from the available metadata and existing record.

One reasonable objection to these findings is that Crowdstrike's excellent cyber protection system, Falcon, was in place prior to July 05, and, therefore, a hack could not have occurred on this date. The locale of the 5th event is in question, whether on a DNC server or later on a copy previously made. True, the action could have been on an earlier copy, in which case Falcon is irrelevant. However, were the action to have occurred on a DNC server then questions arise on the protection granularity decision making criteria of Falcon. For instance, would Falcon stop a DNC user with privileged access, e.g., System Programmer or even a regular authorized user, from copying / downloading something? Here, the conclusion is that it was a local copy, so this question is relevant.

NON-STATE PLAYERS

Interesting that in all the hype about Russiagate with high levels of certainty being that Russia was the perpetrator of the alleged election hacks, there have been no other potential candidates even mentioned. Strange, in that nothing was actually traced back to Russia.

Such is a glaring omission for those aware of the world of non-State players. In addition to other major national intelligence agencies, there is a set of very highly financed, highly intelligent, highly motivated, non-state players with far less at risk and more to gain than Russia. And, there is not a single element of the alleged case against Russia, for instance, that could not have been created or used by a non-state player. Following are facts about one set of non-state players.

They provide fundamental support for the international banking system, the latter dependent upon non-state player's cash flow. They provide support for increased price / earnings ratios of the Market, e.g., Wall Street. They provide support, directly and indirectly, at all levels of federal and local elected officials. Their financial foundation exceeds some nations. Laws are not an impedance to them. From the above, it can be seen that there are incentives to handle with care.

These are the world-wide set of international organized crime (IOC) organizations. The last I heard, their annual profits, from the narcotics trade alone, was in the area of $800,000,000,000 – that's billions. They collectively don't bury this money. It is invested in control.

For instance, elections, both national and local, are very important to their business interests. Their objective is control via leverage, in order to continually increase profits. Profits then lead to more control via leverage. They have the expertise, directly, via leverage, or outright purchase to leverage any type cyber attack which would provide either useful intelligence or influence, for instance, commercial, strategic, or political. The FBI/DHS Grizzly Steppe asserts that one of the "technical indicators" identifying Russia as the perpetrator is as follows "Both groups [APT 28,29] have historically targeted government organizations, think tanks, universities, and corporations around the world." Such an assertion is innocently or deliberately blind to reality, and that it has apparently been accepted by members of our intelligence community is hard to believe.

Where are they, the IOC organizations? The U.S. Russia, Ukraine, Asia, Balkans, Europe, Latin America, wherever.

QUESTIONABLE CONTRACT and FAILURE TO APPEAR

On July 08, 2015 The FBI awarded a no-bid $150,000 contract to Crowdstrike. The reason given for this contract by the FBI was "Urgency." At the same time the contract specifies that there was no "National Interest." An innocent question: How can the FBI have a case of "Urgency" to necessitate a "Non-Competed" contract, and yet there be no "National Interest"? (Source 35)

Dimitri Aperovitch, Crowdstrike Co-founder and Chief Technical Officer and Shawn Henry, Crowdstrike President and Chief Security Officer, appeared on the House Intelligence Committee witness list of March 20, 2017, along with Comey, Rogers, Brennan, Clapper, and Yates. However, Aperovitch and Henry declined to appear. "They declined the invitation, so we're communicating with them about speaking to us privately,' said Jack Langer, a spokesperson for House Intelligence Committee chairman Devin Nunes." (Source 36)

Having been public in findings of Russian culpability of hacking into DNC data, why would these executives not want to have an opportunity to appear before the intelligence committee?

EXPANDED EXPLANATIONS

Source 1: On June 12 2016 Assange of Wikileaks announced "we have upcoming leaks in relation to Hillary Clinton ... we have emails related to Hillary Clinton which are pending publication. That is correct." Just three days later, June 15, "Crowd Strike update a report on malware that they found on the DNC's server ... evidence suggests the malware was injected by Russians." On same day, June 15, a persona Guccifer 2.0 is announced. "... steps forward, calling himself Guccifer2.0 and claiming responsibility for the hack. ... affirms the DNC statement and claims to be a source for Wikileaks. The first 5 documents he posts are purposefully tainted with 'Russian Fingerprints' ... "

Source 2: "... the fingerprints in Guccifer 2.0's first 3 files [as example] were created ... starting off with a blank template (with Russian style sheet attached) saved as 3 pre-tainted template files (with content from real documents copied and pasted into them in separate revision save sessions at a later time). ... In all 3 documents, the same Russian [language 1049] stylesheet definition exists with the same RSID (Revision Save ID) ... means that they all were based on the same document at some point. >From this, we can conclude that all 3 documents were based off an original document that already had "Russian-fingerprints" associated with it and the content was added to each in a separate revision save session."

"If they were separate documents that had these specific "Russian-fingerprints" accidentally added while being handled – they would all have different RSIDs. – The only way for what we observe to have happened [they all have the same RSID] is for all 3 files to be constructed starting off as a pre-tainted template document. Would Russia REALLY apply Russian fingerprints on purpose to leaked files like this?"

Source 3: "This initial copying activity was done on a system where Eastern Daylight Time (EDT) settings were in force. Most likely, the computer used to initially copy the data was located somewhere on the East Coast ... [also] The computer system where the working directories were built had Eastern Daylight Time (EDT) settings in force. Most likely, this system was located somewhere on the East Coast."

Source 4: " ... it's' clear that meta-data was deliberately altered and documents were deliberately pasted into a 'Russianified' word document with Russian language settings and style headings. None of the textual content in any of these four 'poorly sanitised' documents has been altered, removed, or doctored. ... all the differences you would expect from a copy and paste from one editor to another. So why bother copy and pasting into a new document at all? ... So I think we can say for certain that the author wanted the Russian elements to be found. Like, really desperately by the looks of things."

Source 29: Guccifer 2.0's First Five Documents: The Process: This post goes into exact detail. For those interested, visit the web site. It starts as follows: " ... here are processes that appear to have been used to construct Guccifer 2.0's first 5 documents (very likely starting at 1:38pm on June 15th ... not an essential point for the sake of proving the fabrication efforts): "1.doc", "2.doc" & "3.doc" (Probable Procedure)- Based on the version numbers and editing time, it now seems the most probable procedure involved the following: ..."

SOURCES

There are additional detailed cyber forensic reports as sub-reports within some of the following sources.
Source A: GRIZZLY STEPPE – Russian Malicious Cyber Activity
December 29, 2016
https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Source B: Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections
January 6, 2017
https://www.dni.gov/files/documents/ICA_2017_01.pdf

Source 1: Guccifer 2.0: Game Over
July 9, 2017
http://g-2.space/

Source 2: Guccifer 2.0's Multi-Stage Fingerprint Fabrications: RSIDs
June 2, 2017
http://g-2.space/intent/

Source 3: Forensicator – Guccifer 2.0 NGP/VAN Metadata Analysis
July 9, 2017
https://theforensicator.wordpress.com/guccifer-2-ngp-van-metadata-analysis/

Source 4: Russia and WikiLeaks: The Case of the Gilded Guccifer
February 17, 2017
https://medium.com/@nyetnyetnyet/russia-and-wikileaks-the-case-of-the-gilded-guccifer-f2288521cdee

Source 5: The Forensicator – Guccifer 2.0 NGP/VAN Metadata Analysis
August 3, 2017
https://theforensicator.wordpress.com/2017/08/01/the-need-for-speed/

Source 6: ISPS speed report of August 2016: speedtest.net – reports – united-states (link below)
August 3, 2016
http://www.speedtest.net/reports/united-states/

Source 7: US Govt Data Shows Russia Used Outdated Ukrainian PHP Malware
December 30, 2016
https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/

Source 8: Election Hack Report FAQ: What You Need to Know
January 02, 2017
https://www.wordfence.com/blog/2017/01/election-hack-faq/

Source 9: Russian Cyber Attacks in the United States Will 'Intensify
June 15, 2016
http://www.atlanticcouncil.org/about/experts/list/dmitri-alperovitch

Source 10: No real proof in 'Russian hacking' report, as it lacks crucial details ...
December 31, 2016
https://www.rt.com/op-edge/372372-russia-hack-nsa-director/

Source 11: US intel report shoots the messenger to distract from message
January 07, 2017
https://www.rt.com/op-edge/372876-intelligence-report-shoots-messenger

Source 12: Publicly Available Evidence Doesn't Support Russian Gov Hacking of 2016 Election
July 10, 2017
http://www.informationclearinghouse.info/47403.htm

Source 13: FBI/DHS Joint Analysis Report: A Fatally Flawed Effort
December 30, 2016
https://medium.com/@jeffreycarr/fbi-dhs-joint-analysis-report-a-fatally-flawed-effort-b6a98fafe2fa

Source 14: Rush to Judgment-The evidence that the Russians hacked the DNC is collapsing
March 24, 2017
http://original.antiwar.com/justin/2017/03/23/rush-to-judgment/

Source 15: Faith-based Attribution
July 10, 2016
https://medium.com/@jeffreycarr/faith-based-attribution-30f4a658eabc

Source 16: Cyber security Firm Finds Evidence that Russian Military Unit Was Behind DNC Hack
December 22, 2016
https://www.washingtonpost.com/world/national-security/cybersecurity-firm-finds-a-link-between-dnc-hack-and-ukrainian-artillery/2016/12/21/47bf1f5a-c7e3-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.8456d13277a7

Source 17: Use of Fancy Bear Android Malware in Tracking of Ukrainian Military Field Artillarey Units
December 22, 2016 updated March 23, 2017
https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/

Source 18: Security Company Releases New Evidence of Russian Role in DC Hack
December 22, 2016
http://www.pbs.org/newshour/bb/security-company-releases-new-evidence-russian-role-dnc-hack/

Source 19: Skeptics Doubt Ukraine Hack, Its Link to DNC Cyberattack
December 22, 2016
https://www.voanews.com/a/skeptics-doubt-ukraine-hack-link-to-dnc-cyberattack/3649234.html

Source 20: Dissection of Sednit Espionage Group
October 20, 2016

https://www.eset.com/us/about/newsroom/press-releases/dissection-of-sednit-espionage-group-1/

Source 21:Think Tank: Cyber Firm at Center of Russian Hacking Charges Misread Data
March 23, 2017
https://www.voanews.com/a/crowdstrike-comey-russia-hack-dnc-clinton-trump/3776067.html

Source 22: Is Skepticism Treason?
January 3, 2017
https://www.thenation.com/article/is-skepticism-treason/

Source 23: Allegedly' Disappears as Russians Blamed for DNC Hack
June 16, 2016
http://fair.org/home/allegedly-disappears-as-russians-blamed-for-dnc-hack/

Source 24: Marble Framework
March 31, 2017
https://wikileaks.org/vault7/#Athena

Source 25: Julian Assange: Our source is not the Russian government
January 3, 2017
http://www.foxnews.com/transcript/2017/01/03/julian-assange-our-source-is-not-russian-government/

Source 26: CrowdStrike, Comey & Conflicting Claims?
July 16, 2017
http://g-2.space/diskimg/

Source 27: Full text: James Come testimony transcript on Trump and Russia
June 8, 2017
http://www.politico.com/story/2017/06/08/full-text-james-Come-trump-russia-testimony-239295

Source 28: Hacked computer server that handled DNC email remains out of reach of Russia investigators
July 5, 2017
http://www.washingtontimes.com/news/2017/jul/5/dnc-email-server-most-wanted-evidence-for-russia-I/

Source 29: Guccifer 2.0's First Five Documents: The Process
May 31, 2017
http://g-2.space/process/

Source 30: Timeline
http://g-2.space/timeline.html

Source 31: Clinton Charity Tapped Foreign Friends
March 19, 2015
https://www.wsj.com/articles/clinton-charity-tapped-foreign-friends-1426818602

Source 32:
https://twitter.com/GUCCIFER_2/status/750054910083883008
https://guccifer2.wordpress.com/2016/07/06/trumpocalypse/

Source 33: Distortions & Missing The Point (feat. The Washington Post, The Hill, Sam Biddle & Matt Tait)
August 16, 2017
http://g-2.space/distortions/

Source 34: Assange meets US congressman, vows to prove Russia did not leak him documents
August 16, 2017
http://thehill.com/policy/cybersecurity/346904-assange-meets-us-congressman-vows-to-prove-russia-did-not-leak-him

Source 35: AWARD SUMMARY, – CROWDSTRIKE INC.
July 8, 2015
https://www.usaspending.gov/Transparency/Pages/AwardSummary.aspx?AwardID=44480195

Transaction details
https://www.usaspending.gov/transparency/Pages/TransactionDetails.aspx?RecordID=EEFBF110-EC44-4308-8C6F-F171909722AF&AwardID=44480195&AwardType=C

Source 36: Cybersecurity experts ... refuse to co-operate with Congress
April 5, 2017
http://www.dailymail.co.uk/news/article-4376628/New-questions-claim-Russia-hacked-election.html

Source 37: James Clapper address to the National Press Club
June 8, 2017
http://www.anu.edu.au/news/all-news/speech-professor-james-clapper-ao-address-to-the-national-press-club

Source 38: James Clapper NBC Meet the Press –
May 28, 2017
https://www.nbcnews.com/meet-the-press/meet-press-may-28-2017-n765626

Source 39: New Cracks in Russia-gate 'Assessment'
May 23, 2017
https://consortiumnews.com/2017/05/23/new-cracks-in-russia-gate-assessment/

Source 40: The TV5 MONDE Hack of APT28
October 10, 2017
https://climateaudit.org/2017/10/10/part-2-the-tv5-monde-hack-and-apt28/

Source 41: Bears in the Mist: Intrusion into the Democratic National Committee
June 15, 2016
https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Source 42: Did CrowdStrike Engage In A Clandestine Leak Investigation?
November 27, 2017
http://g-2.space/cs2/

Source 43: Hunting the DNC hackers: how Crowdstrike found proof Russia hacked ...
March 5, 2017
http://www.wired.co.uk/article/dnc-hack-proof-russia-democrats

Source 44: Duncan Campbell's Hit-Piece ... Fake News Fueled By RussiaGate Derangement
December 27th, 2017
http://g-2.space/thereg *(note: If password is requested, use "12939")*

Source 45: Built To Stop Breaches – Falcon Host
https://web.archive.org/web/20160428142131/https://www.crowdstrike.com/products/

Source 46: Did CrowdStrike Engage In A Clandestine Leak Investigation?
November 27, 2017
http://g-2.space/cs2/

Source 47: DHS Official Denies Russia Tried to Hack 21 State Voting Systems
November 29 2017
https://www.c-span.org/video/?c4700287/dhs-official-denies-russia-hack-21-state-voting-systems

Source 48: Fancy Frauds, Bogus Bears & Malware Mimicry?!
December 26 2017
https://disobedientmedia.com/2017/12/fancy-frauds-bogus-bears-malware-mimicry/

This report is an enclosure to the August 21, 2017 submission to the Office of Special Council, titled "Subject: Non-Existent Foundation for Russian Hacking Charge"

Skip Folden, Independent – non-affiliated

This report has been received by the offices of Special Council Mueller, Deputy Attorney General Rod J. Rosenstein, as well as House and Senate Intelligence and Judiciary Committees and the White House Chief of Staff.

The report has been submitted in response to the Dec. 29, 2016 Grizzly Steppe and Jan. 06, 2017 ICA reports. If you take exception with this report and feel that you can be of assistance to the intelligence agencies in responding, you may submit to the Office of Special Council, Deputy Attorney General, and / or the House and Senate Intelligence Committees and Senate Judicial Committee.

If you support this report, you may consider writing or phoning any of the named committees and expressing your support. In either case, thank you for taking the time to read such a lengthily report.

ADDENDUM SUPPLEMENT – December 31, 2017

Subjects:
1) Report context – cover letter
2) Current Transatlantic capacity tests
3) Time Zone of July 05 2016 incident
4) Crowdstrike Falcon DNC monitoring Total Silence on mail loss – missed?
5) Evolutionary Considerations of APT28
6) Using targets to define attribution
7) Alperovitch linking DNC intrusion to France's TV5 Monde TV station incursion
8) Clapper and Russian genetic code assertions
9) Clapper and "two dozen or so analysts"
10) DHS refutes accusation Russia hacked voting systems
11) Suspicious Compile dates and a hard coded IP address possibly inoperable

---

1) Report context – cover letter
For those who have read this report herein is added the context. To federal addressees, e.g., Office of Special Council, Assistant Attorney General, etc., the following requests were made. Note right off the top, the request to first verify the report contents with the suggestion of using the FBI Forensic experts. In other

words, the addressees were not asked to take the discoveries of the report without verifying. Further, this report was held from the public until 1) USPS verified that all copies had been delivered to the addresses and 2) that a week had passed since receipt, in order to give time to acknowledge that receipt, prior to allowing the report into the public. This was as a courtesy to the addressees to give an opportunity of a heads-up.

——————— from cover letter ———————-

Please have federal investigators, e.g., FBI cyber forensics, verify the findings of this report, each of which includes well qualified sources. The requested investigations also stem from this report.
VERIFY: (Subjects covered in enclosed report)
1) Findings identified in Lack of Grizzly Steppe Foundations
2) No discovered connection between Russia and Wikileaks
3) Recent metadata discoveries by independent cyber forensic experts
4) Validity of missing Disclosures and violation of assessment requirements
5) Crowdstrike's use of failed Ukrainian Howitzer hack charge to raise Fancy Bear / GRU confidence level to High
6) Crowdstrike's possible potential conflicts of interest
INVESTIGATE
1) Refusal of DNC to allow FBI to access to DNC server(s)
2) Failure of FBI to pursue access to DNC server(s)
3) Identified major coincidences of timing of events of June 12,14 and 15 2016
4) FBI – Crowdstrike July 08, 2015, no-bid, urgent, no-national interest, contract
5) Potential collusion(s) to intentionally mislead in effort to weaken or bring down the president or falsely blame Russia in pursuit of a pre-determined policy.
PROSECUTE
1) As threat to national security, any findings of collusion to blame Russia. The resultant deterioration of US – Russian relations due to interference assertions is leading to potential war, and that clearly is a threat to our national security.
2) As threat to national security, any findings of collusion to weaken or remove the president. The severe disruption to our government which has occurred and would escalate, along with probable increased citizen upheavals would further weaken our nation and is clearly a threat to our national security.

2) Current (November 2017) trans-Atlantic capacity speed test results (email 11/29/17)

Related Report Section: the CYBER-FORENSIC CONCLUSIONS

These post-report tests were performed by Bill Kinney (US) and Duncan Campbell (UK)

These results are in MegaBytes – not MegaBits.

.8 mBps on a 100 mbps line in a home in Amsterdam

1.6 mBps on a commercial DSL in Amsterdam

12 mBps between data centres in New Jersey and the UK

From Belgrade and Albania did not even try – line rates were just too slow

The top transfer rate of the 05 July incident was 49.1 mBps and most conservative approach being a 38 MB/s observation, because it was over a large sequence of data with no intervening gaps

The best transfer speed capacity found in these tests was only approx. 25% – 30% of that which would have been required for the 05 July incident to have been a cross Atlantic cyber intrusion.
The finding, again, was, "The data was a download not a long-distance hack. and The download is compatible with a USB thumb drive"

---

3) Time Zone of July 05 2016 incident
Related Report Sections:
CYBER-FORENSIC CONCLUSIONS
EXPANDED EXPLANATIONS
Questions continue to be raised about the validity of the conclusion of the July 05 incident having occurred in the Eastern Time Zone.
For instance, "could have been done anywhere in the world, on any date and at any time between 1 January 2012 and 8 September 2016."
Yes, perhaps, but hypothetical.
Anywhere in the world?: Does or doesn't a local copy to a thumb drive require either the copied source to be at the same geographical location as the thumb drive or within band-width capacity of the thumb drive? The Atlantic did not support the required capacity. Did the Pacific? Did the DNC computer topography include locations across both the Atlantic and Pacific oceans?
Between 1 January 2012 ...? Are there no records within any of the files containing references to events which occurred after 1 January 2012? The point is the assertion appears a bit broad.
Adam Carter (source 44)
"There are other possibilities but they are far less likely, with all 9 files in the top level archive having minutes that fall neatly in to the range in minutes of all the other files transferred on the same date (where the hours displayed don't change due to timezone) in the way that they do – it makes it a significantly high probability the files were archived in Eastern Time zone."
The report clearly states the following:
Forensicator: " ... any conclusions reached from an analysis activity will be balance of hard facts and judgements based on experience and perceived probabilities and plausibilities ..."
Forensicator: "Timezone remained set as Eastern time throughout all dates of transfers and while system clocks and locale settings can, of course, be changed – it would be illogical for someone claiming to be in Romania – to set their timezone to something that would then contradict it."

---

4) Crowdstrike Falcon DNC monitoring Total Silence on mail loss – missed?
Related Report Sections:
MISSING LINK BETWEEN WIKILEAKS AND RUSSIA
HIGHLY COINCIDENTAL TIMING
EXPANDED EXPLANATIONS

(source 46) By May 12 2016 Crowdstrike had Falcon installed on all computers of DNC.
The last email released by Wikileaks was dated May 25 2016.
During that approx. two weeks Falcon was at least monitoring if not stopping all malware intrusions.
Crowdstrike has neither disclosed nor mentioned "evidence of email acquisition" during this period. Missed, never occurred, or with-holding information?
(source 45): Falcon Description: "Continuous visibility protects your endpoints against all threat types — known and unknown, malware and malware-free. Nothing is missed, so you can respond in real-time to stop breaches." What's that again, "Nothing is missed"?

---

5) Evolutionary Considerations of APT28, aka Fancy Bear, Sofacy, Strontium, Sednit group, etc.
Related Report Section: LACK OF GRIZZLY STEPPE FOUNDATIONS
My assessment of the status of APT28 by whatever name.
Whatever logic was initially used over ten years ago to attribute to Russian intelligence the expertise, tools and facilities used by APT28 cannot be assumed to still hold. Too much time has passed in the context of ever-increasing world-wide cyber sophistication. Nothing remains constant.
Some cyber protection companies still automatically attribute APT28 to the Russian Military Intelligence group GRU. It is not impossible that such is sometimes the case. However, other than the apparent fact that APT28 has never been trace routed to Russia, let alone the GRU, too many years have passed to assume nothing has changed since the original assumptive attribution to Russia.
More than ten years ago there was an original unknown entity which was recognized as using a particular set of tools, procedures, facilities, expertise, etc., and it was given various names, one of which became Fancy Bear, purposefully named for its implication, by Crowdstrike.
As time progressed, these tools, and those later appearing as zero day, etc., lost their original exclusivity to any one player. As each new tool, etc., was launched, it soon or eventually became or would become non-exclusive. Such meant it was or would be available for other world-wide entities with sufficient technical expertise, whether they be state or non-state.
The APT28 combination of capabilities or sub-sets by this time is likely used by a non-consistent set of international state and non-state players, the latter being governmental and non-governmental organizations or groups.
World-wide entities with potentially sufficient expertise currently capable of using capabilities of APT28 could include, as examples only, state players such as Albania, Brazil, Britain, China, Germany, Hungry, India, Italy, Romania, Russia, Taiwan, Turkey, U.S., Ukraine, etc. The potential non-state players are unknown, but could certainly include major International Organized Crime organizations with immense resources and the necessary profit and political control motives.

---

6) Using targets to define attribution

Related Report Section: LACK OF GRIZZLY STEPPE FOUNDATIONS

Some cyber protection companies use cyber intrusion targets as rationale for Russian attribution.

Such a foundation for attribution of cyber intrusion is weak.

Cyber intrusion targeted facilities, such as government organizations, elections, think tanks, financial institutions, universities, corporations, infrastructures, etc., can be of interest to many world-wide sponsors of cyber attack groups, depending on the subject and timing, for political or financial leverage. None of the targets attributed to Russia are of potential interest to only Russia.

For instance, as stated in above report, Grizzly Steppe, page 2, second paragraph, states as proof of Russian guilt, "Both groups [APT28 and 29] have historically targeted government organizations, think tanks, universities, and corporations around the world." None of these targets can be claimed as unique to Russian interest, or which exclude any other state or major non-state group.

We know our CIA does exactly that to other nations, and it's certainly not alone. Our presidential election outcomes are of significant interest, from perspectives of national security and financially, to most other nations as well as some well financed non-state players.

Any potential cyber target in which Russia has an interested, the US, England, and NATO at minimum would most likely share that interest for their own purposes.

It is fallacious to think that only Russia would be interested in given potential target lists. For instance, Ukraine has been identified as a Russia only target. We spent five billion dollars and had direct involvement in the overthrow of their elected government. That qualifies as interest.

Also, any Russian individual active in opposing Putin would qualify for our interest, etc. So, the theme, assertion, assumption that a given subject list could only be of interest to the "Kremlin" is nonsense.

---

7) Alperovitch linking DNC intrusion to France's TV5 Monde TV station in April 2015 via APT28. (Sources 40, 41)

Related Report Section: PREVIOUS RUSSIAN ACCUSATIONS REFUTED

Alperovitch alleged a link between Fancy Bear as used against DNC and the 2015 extensive intrusion into France's TV5 Monde TV..

Alperovitch: "FANCY BEAR (also known as Sofacy or APT 28) is a separate Russian-based threat actor, which has been active since mid 2000s ... FANCY BEAR has also been linked publicly to intrusions into ... France's TV5 Monde TV station in April 2015."

APT28 was not definitively linked to the TV5 massive intrusion. This assertion was based on the theory that Russia used a cyber false flag operation to point to CyberCaliphate. The latter had not only claimed responsibility, but the claim reportedly had supporting evidence. Alperovitch made his claim as if such a link to APT28 had been established. It had not. It was only one theory that the TV5 attack was a Russian false flag.

There had been possible IP overlap between CyberCaliphate and APT28, which overlap apparently was never identified. The purported IP overlap was used to jump to the conclusion that the CyberCaliph attack was really an APT28 false flag. However, IP overlap is not conclusive of anything. Further, use of a Cyrillic keyboard and code being compiled during office hours in Moscow and St. Petersburg were falsely attributed to this attack, whereas those two attributions actually applied to a different earlier attack of Oct 14 2014.
As pointed out by McIntyre it ranges from very difficult to impossible to find any google search reference to the original attribution of the TV5 attack to CyberCaliphate, but only stories attributing the attack to Russia. That is a good example of a google search algorithm using misdirection and thereby misrepresenting the story so as to point only to Russia. It is also a case of Alperovitch having selective memory.

8) Clapper and Russian genetic code assertions (Sources 37,38)
Related Report Section: ICA REPORT
Following are examples of the type of psychotic assumptions which formed the basis of the Jan 06 ICA. James Clapper was the Director of National Intelligence for the Jan 06 2017 ICA and selector of those agents who authored the report.
James Clapper, National Press Club, June 08 2017:
"... as far as our being intimate allies, trusting buds with the Russians that is just not going to happen. It is in their genes to be opposed, diametrically opposed to the United States and to Western democracies."
James Clapper, NBC Meet the Press, May 28 2017:
"... just the historical practices of the Russians, who typically, almost genetically driven to co-opt, penetrate, gain favor, whatever, which is a typical Russian technique. ...."

9) Clapper and "two dozen or so analysts" (Source 39)
Related Report Section: IC-COORDINATED ASSESSMENT
James Clapper, Senate Judiciary subcommittee, May 8 2017: "the two dozen or so analysts for this task were hand-picked, seasoned experts from each of the contributing agencies."

10) DHS refutes accusation Russia hacked voting systems (source 47)
It was widely reported by main media that Russia hacked the voting systems of 21 states.
On December 21 2017, Christopher Kerbs, cyber-security official of Homeland Security, testified to Congress that no hacking occurred:
"The majority of the activity was simple scanning. ... Scanning is a regular activity across the Web. I would not characterize that as an attack.... If that context was not provided, I apologize. ... When we talk about that scanning, it was not also necessarily an election system that was scanned.

11) Suspicious Compile dates and a hard coded IP address possibly inoperable (source 48)

Related Report Section: LACK OF GRIZZLY STEPPE FOUNDATIONS

CrowdStrike in its analysis of the purported DNC intrusion by Russia, identified three indicators of compromise (IOC) attributed to APT28, Fancy Bear. Two of these IOCs (X-tunnel implant and 64-bit X-agent implant) actually had compile dates concurrent with Crowdstrike's presence at DNC (May 05 (Crowdstrike first consulting visit) and 10 2016 (just prior to installation of Falcon). That should raise eye-brows. The third had a compilation date only about two weeks prior (April 25 2016) to Crowdstrike's presence.

Compile timestamps can be manipulated. However, "Invincea (part of Sophos) have inspected many malware samples as part of a case study looking at malware compile times. ...They found that generally, in a lot of cases, malware developers didn't care to hide the compile times and that while implausible timestamps are used, it's rare that these use dates in the future."

It's most likely even far more rare that two dates set in the future for some reason would coincide with the presence of Crowdstrike.

So, what take away question does malware compilation dates coincide with Crowdstrike's presence raise? Did Crowdstrike possibly plant malware and then immediately claim a Russian intrusion?

Further, to add another incongruent facet to the overly rapid attribution to Russia is that the purported DNC malware contained a hard-coded IP address, also used to ID Fancy Bear.

The problem, however, is that this hard-coded IP address had been disabled by the owner almost one year prior to the alleged DNC intrusion. It has not yet been established that this IP address was re-activated in the mean time. As the site owner was very upset at it having been possibly used for malicious purpose by Fancy Bear, it is more unlikely than not that he would have had it re-activated so it could be used maliciously again by the same party.

Was a long inoperable IP address included in the 'discovered' malware as well as the two compile dates coinciding with the presence of Crowdstrike?