GlobalResearch
Center for Research on Globalization

Rush to Judgment. The Russian Hacking Saga

The evidence that the Russians hacked the DNC is collapsing

By Justin Raimondo
Global Research, March 26, 2017
Anti War 24 March 2017

Region: Russia and FSU, USA
Theme: Intelligence

The allegation – now accepted as incontrovertible fact by the "mainstream" media – that the Russian intelligence services hacked the Democratic National Committee (and John Podesta's emails) in an effort to help Donald Trump get elected recently suffered a blow from which it may not recover.

Crowdstrike is the cybersecurity company hired by the DNC to determine who hacked their accounts: it took them a single day to determine the identity of the culprits – it was, they said, two groups of hackers which they named "Fancy Bear" and "Cozy Bear," affiliated respectively with the GRU, which is Russian military intelligence, and the FSB, the Russian security service.

How did they know this?

These alleged "hacker groups" are not associated with any known individuals in any way connected to Russian intelligence: instead, they are identified by the tools they use, the times they do their dirty work, the nature of the targets, and other characteristics based on the history of past intrusions.

Yet as Jeffrey Carr and other cyberwarfare experts have pointed out, this methodology is fatally flawed.

"It's important to know that the process of attributing an attack by a cybersecurity company has nothing to do with the scientific method," writes Carr:

> "Claims of attribution aren't testable or repeatable because the hypothesis is never proven right or wrong. Neither are claims of attribution admissible in any criminal case, so those who make the claim don't have to abide by any rules of evidence (i.e., hearsay, relevance, admissibility)."

Likening attribution claims of hacking incidents by cybersecurity companies to intelligence assessments, Carr notes that, unlike government agencies such the CIA, these companies are never held to account for their misses:

> "When it comes to cybersecurity estimates of attribution, no one holds the company that makes the claim accountable because there's no way to prove whether the assignment of attribution is true or false unless (1) there is a criminal conviction, (2) the hacker is caught in the act, or (3) a government employee leaked the evidence."

This lack of accountability may be changing, however, because Crowdstrike's case for attributing the hacking of the DNC to the Russians is falling apart at the seams like a cheap sweater.

To begin with, Crowdstrike initially gauged its certainty as to the identity of the hackers with "medium confidence." However, a later development, announced in late December and touted by the *Washington Post*, boosted this to "high confidence." The reason for this newfound near-certainty was their discovery that "Fancy Bear" had also infected an application used by the Ukrainian military to target separatist artillery in the Ukrainian civil war. As the *Post* reported:

> "While CrowdStrike, which was hired by the DNC to investigate the intrusions and whose findings are described in a new report, had always suspected that one of the two hacker groups that struck the DNC was the GRU, Russia's military intelligence agency, it had only medium confidence.
>
> "Now, said CrowdStrike co-founder Dmitri Alperovitch, 'we have high confidence' it was a unit of the GRU. CrowdStrike had dubbed that unit 'Fancy Bear.'"

Crowdstrike published an analysis that claimed a malware program supposedly unique to Fancy Bear, X-Agent, had infected a Ukrainian targeting application and, using GPS to geo-locate Ukrainian positions, had turned the application against the Ukrainians, resulting in huge losses:

> "Between July and August 2014, Russian-backed forces launched some of the most-decisive attacks against Ukrainian forces, resulting in significant loss of life, weaponry and territory.
>
> "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 told the PBS News Hour that

> "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."

He told NBC News that this proved the DNC hacker "wasn't a 400-pound guy in his bed," as Trump had opined during the first presidential debate – it was the Russians.

The only problem with this analysis is that is isn't true. It turns out that Crowdstrike's estimate of Ukrainian losses was based on a blog post by a pro-Russian blogger eager to tout Ukrainian losses: the Ukrainians denied it. Furthermore, the hacking attribution was based on the hackers' use of a malware program called X-Agent, supposedly unique to Fancy Bear. Since the target was the Ukrainian military, Crowdstrike extrapolated from this that the hackers were working for the Russians.

All somewhat plausible, except for two things: To begin with, as Jeffrey Carr pointed out in December, and now others are beginning to realize, X-Agent isn't unique to Fancy Bear. Citing the findings of ESET, another cybersecurity company, he wrote:

> "Unlike Crowdstrike, 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 again and again by anyone. In other words – malware deployed is malware enjoyed!
>
> "In fact, the source code for X-Agent, which was used in the DNC, Bundestag, and TV5Monde attacks, was obtained by ESET as part of their investigation!
>
> "During our investigations, we were able to retrieve the complete Xagent source code for the Linux operating system…."
>
> "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."

Secondly, the estimate Crowdstrike used to verify the Ukrainian losses was supposedly based on data from the respected International Institute for Strategic Studies (IISS). But now IISS is disavowing and debunking their claims:

> "[T]he International Institute for Strategic Studies (IISS) told [Voice of America] that CrowdStrike erroneously used IISS data as proof of the intrusion. IISS disavowed any connection to the CrowdStrike report. Ukraine's Ministry of Defense also has claimed combat losses and hacking never happened….
>
> "'The CrowdStrike report uses our data, but the inferences and analysis drawn from that data belong solely to the report's authors," the IISS said. "The inference they make that reductions in Ukrainian D-30 artillery holdings between 2013 and 2016 were primarily the result of combat losses is not a conclusion that we have ever suggested ourselves, nor one we believe to be accurate.'
>
> "One of the IISS researchers who produced the data said that while the think tank had dramatically lowered its estimates of Ukrainian artillery assets and howitzers in 2013, it did so as part of a 'reassessment" and reallocation of units to airborne forces.'
>
> "'No, we have never attributed this reduction to combat losses," the IISS researcher said, explaining that most of the reallocation occurred prior to the two-year period that CrowdStrike cites in its report.
>
> "'The vast majority of the reduction actually occurs … before Crimea/Donbass,' he added, referring to the 2014 Russian invasion of Ukraine."

The definitive "evidence" cited by Alperovitch is now effectively debunked: indeed, it was debunked by Carr late last year, but that was ignored in the media's rush to "prove" the Russians hacked the DNC in order to further Trump's presidential ambitions. The exposure by the Voice of America of Crowdstrike's falsification of Ukrainian battlefield losses – the supposedly solid "proof" of attributing the hack to the GRU – is the final nail in Crowdstrike's coffin. They didn't bother to verify their analysis of IISS's data with IISS – they simply took as

gospel the allegations of a pro-Russian blogger. They didn't contact the Ukrainian military, either: instead, their confirmation bias dictated that they shaped the "facts" to fit their predetermined conclusion.

Now why do you suppose that is? Why were they married so early – after a single day – to the conclusion that it was the Russians who were behind the hacking of the DNC?

Crowdstrike founder Alperovitch is a Nonresident Senior Fellow of the Atlantic Council, and head honcho of its "Cyber Statecraft Initiative" – of which his role in promoting the "Putin did it" scenario is a Exhibit A. James Carden, writing in *The Nation*, makes the trenchant point that

> "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, writing on the FAIR blog, adds to our knowledge by noting that the Council's budget is also supplemented by "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)."

Johnson also notes that CrowdStrike currently has a $150,000 / year, no-bid contract with the FBI for "systems analysis."

Nice work if you can get it.

This last little tidbit gives us some insight into what is perhaps the most curious aspect of the Russian-hackers-campaign-for-Trump story: the FBI's complete dependence on Crowdstrike's analysis. Amazingly, the FBI did no independent forensic work on the DNC servers before Crowdstrike got its hot little hands on them: indeed, the DNC denied the FBI access to the servers, and, as far as anyone knows, the FBI never examined them. BuzzFeed quotes an anonymous "intelligence official" as saying "Crowdstrike is pretty good. There's no reason to believe that anything they have concluded is not accurate."

There is now.

Alperovitch is scheduled to testify before the House Intelligence Committee, and one wonders if our clueless – and technically challenged – Republican members of Congress will question him about the debunking of Crowdstrike's rush to judgment. I tend to doubt it, since the Russia-did-it meme is now the Accepted Narrative and no dissent is permitted – to challenge it would make them "Putin apologists"! (Although maybe Trey Gowdy, the only GOPer on that panel who seems to have any brains, may surprise me.)

As I've been saying for months, there is no evidence that the Russians hacked the DNC: none, zilch, nada. Yet this false narrative is the entire basis of a campaign launched by the Democrats, hailed by the Trump-hating media, and fully endorsed by the FBI and the CIA, the purpose of which is to "prove" that Trump is "Putin's puppet," as Hillary Clinton put it. Now the investigative powers of the federal government are being deployed to confirm

that the Trump campaign “colluded” with the Kremlin in an act the evidence for which is collapsing.

This whole affair is a vicious fraud. If there is any justice in this world – and there may not be – the perpetrators should be charged, tried, and jailed.

NOTES IN THE MARGIN

You can check out my Twitter feed by going here. But please note that my tweets are sometimes deliberately provocative, often made in jest, and largely consist of me thinking out loud.

I’ve written a couple of books, which you might want to peruse. Here is the link for buying the second edition of my 1993 book, Reclaiming the American Right: The Lost Legacy of the Conservative Movement, with an Introduction by Prof. George W. Carey, a Foreword by Patrick J. Buchanan, and critical essays by Scott Richert and David Gordon (ISI Books, 2008).

You can buy An Enemy of the State: The Life of Murray N. Rothbard (Prometheus Books, 2000), my biography of the great libertarian thinker, here.

Articles by: Justin Raimondo