

DNC Refused to Give FBI Access to Its Servers ... Instead Gave Access to a DNC Consultant Tied to Organization Promoting Conflict with Russia

By [Washington's Blog](#)

Global Research, January 06, 2017

[Washington's Blog](#) 5 January 2017

Region: [USA](#)

Theme: [Intelligence](#)

In-depth Report: [Election Fraud in America](#),
[U.S. Elections](#)

CNN [reports](#):

The Democratic National Committee “rebuffed” a request from the FBI to examine its computer services after it was allegedly hacked by Russia during the 2016 election, a senior law enforcement official told CNN Thursday.

“The FBI repeatedly stressed to DNC officials the necessity of obtaining direct access to servers and data, only to be rebuffed until well after the initial compromise had been mitigated,” a senior law enforcement official told CNN. “This left the FBI no choice but to rely upon a third party for information.

The FBI instead relied on the assessment from a third-party security company called CrowdStrike.

As [first reported](#) by George Eliason, CrowdStrike’s Chief Technology Officer and Co-Founder Dimitri Alperovitch – who [wrote](#) the CrowdStrike reports allegedly linking Russia to the Democratic party emails published by Wikileaks – is a fellow at the Atlantic Council ... an organization associated with Ukraine, and whose *main* policy goal seems to stir up a confrontation with Russia. [1].

The Nation [writes](#):

In late December, Crowdstrike released a [largely debunked](#) report claiming that the same Russian malware that was used to hack the DNC has been used by Russian intelligence to target Ukrainian artillery positions. Crowdstrike’s co-founder and chief technology officer, [Dmitri Alperovitch](#), told PBS, “Ukraine’s artillery men were targeted by the same hackers...that targeted DNC, but this time they were targeting cellphones [belonging to the Ukrainian artillery men] to try to understand their location so that the Russian artillery forces can actually target them in the open battle.”

[Dmitri Alperovitch](#) is also a senior fellow at the Atlantic Council.

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. As I pointed out in the pages of *The Nation* in November, the Atlantic Council has spent the past several years producing some of the most virulent specimens of the new Cold War propaganda.

It would seem then that a healthy amount of skepticism toward a government report that relied, in part, on the findings of private-sector cyber security companies like Crowdstrike might be in order.

The Atlantic Council is also [funded by](#) the U.S. military and the largest defense contractors, including:

- United States Army
- United States Navy
- United States Air Force
- United States Marines
- Lockheed Martin
- Raytheon
- Northrop Grumman
- Boeing

[1] Here's an [example](#) of the Atlantic Council's bellicose rhetoric from July 2016:

Poland should announce that it reserves the right to deploy offensive cyber operations (and not necessarily in response just to cyber attacks). The authorities could also suggest potential targets, which could include the Moscow metro, the St. Petersburg power network, and Russian state-run media outlets such as RT.

The original source of this article is [Washington's Blog](#)
Copyright © [Washington's Blog](#), [Washington's Blog](#), 2017

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Washington's Blog](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca