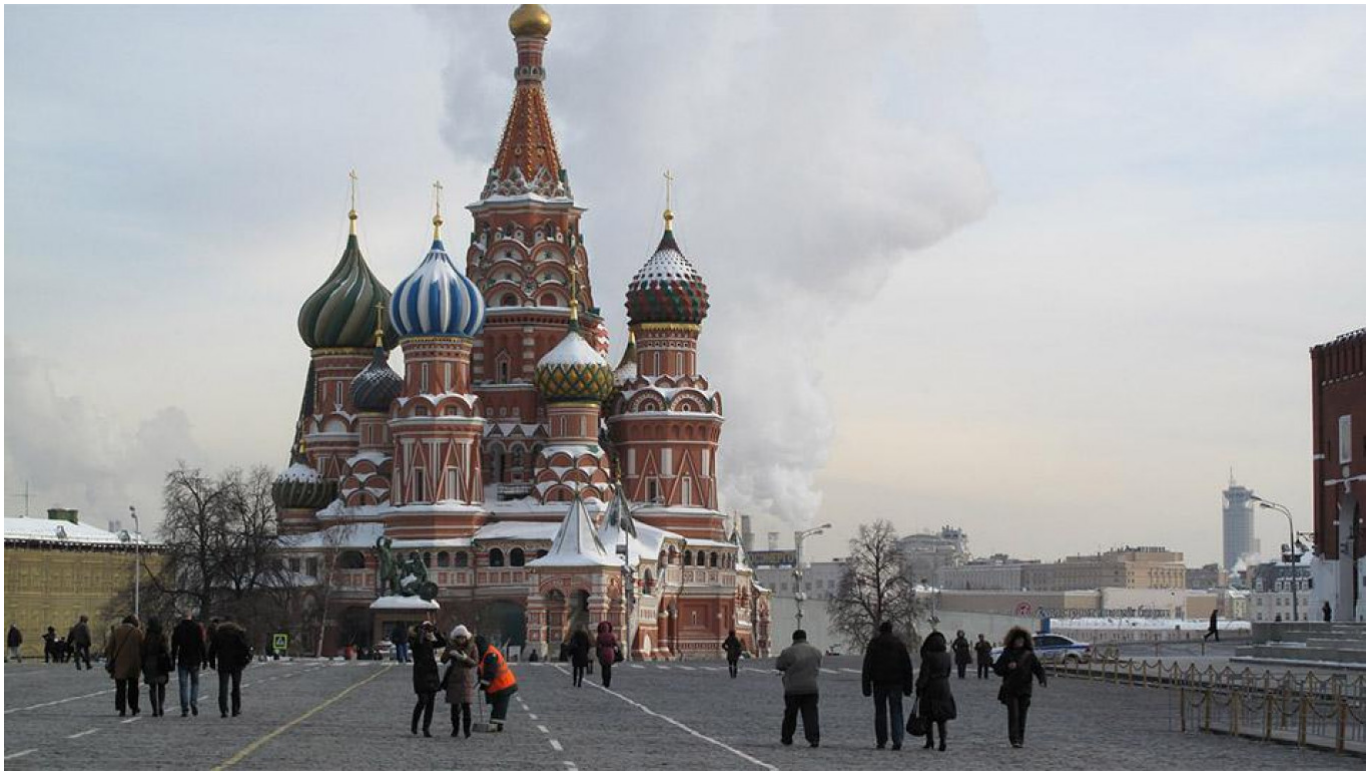
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Release the Dutch Evidence of the Russian DNC Hack (Op-ed)

If the Dutch intelligence service watched the Russians breach the Democratic National Committee, there's no more reason to hide the evidence

By Leonid Bershidsky

January 26, 2018



(Bloomberg View) — For the first time in a year, significant new information has emerged linking the 2016 U.S. Democratic National Committee security breach to Russia. A newspaper in the Netherlands reports that U.S. authorities received evidence of the hack from the Dutch intelligence service, which had penetrated the Russian hackers. The report partly explains the U.S. intelligence community's certainty about what happened to the DNC and its reluctance to tell the public more. But it also raises new questions.

The story in the daily De Volkskrant is based on anonymous sources, as are almost all other substantial reports about Russian interference in the U.S. presidential election. But it provides

enough exciting detail to be a major addition to what's publicly available. According to the paper, hackers from AIVD, the Dutch General Intelligence and Security Service, penetrated the network of the Russian hacker group known as Cozy Bear in the summer of 2014.

Embed:

According to the Dutch story, Cozy Bear, or, to use its generic designation in the cybersecurity community, Advanced Persistent Threat 29, worked from «a space in a university building near the Red Square.» That would fit the description of Moscow State University's historic campus across from Red Square, occupied today by some of its humanities departments and the Institute of Asian and African Countries, which has traditionally sent large numbers of its graduates to the SVR, the Russian foreign intelligence service.

The Dutch hackers, reportedly, didn't just watch everything Cozy Bear — a fluid group in which about 10 people were active at any given time — was doing on its computers. They also took over the security camera that recorded all the comings and goings at the group's space. Dutch intelligence matched the faces of visitors against a database of known Russian agents and linked the group to the SVR. Crowdstrike, the cybersecurity firm retained by the DNC, hinted in its analysis of the breach that Cozy Bear could have been run by either SVR or the FSB, Russia's domestic intelligence service, so the Dutch report clarifies the attribution.

Related article: The Hacker Hunters Chasing Russian Shadows

In November 2014, the Dutch reportedly alerted the U.S. intelligence community that Cozy Bear was attacking the State Department, and helped the National Security Agency thwart the sustained attack. The Volkskrant story also claims that, a year after it first penetrated APT Cozy Bear in the summer of 2015, the Dutch intelligence service witnessed how the Russian hackers launched «an attack on the Democratic Party in the United States.»

U.S. colleagues sent cake and flowers to AIVD headquarters in Zoetermeer in appreciation. But after leaks in U.S. media that a «Western ally» had helped uncover Russian interference in the election, the Dutch became worried that their methods would be disclosed, and they've since scaled down their cooperation with U.S. intelligence services, fearing further leaks. The AIVD hackers are no longer in the Cozy Bear network, and the story says their ability to track the Russian group lasted between a year and 2.5 years.

If the story is correct, it explains why the U.S. intelligence community's assessment of Russian interference provided scant evidence. If the information came from AIVD, the secrets weren't the Americans' to disclose. It also explains why the Federal Bureau of Investigation, by its own admission, never examined the DNC servers that had been penetrated, seemingly relying on data from Crowdstrike. If it had all the technical evidence from the Dutch, it may not have needed to look at the servers.

Related article: Inside A Hacker's Mind

But the questions raised by the Dutch scoop are as significant as the gaps it helps to close.

If the Dutch witnessed the DNC intrusion in 2015 and reported it to U.S. colleagues, it's difficult to understand why the Russian hackers were left to forage in the DNC network for months without being ejected. After all, Cozy Bear's attacks on the State Department and the White House were actively fought as soon as they became apparent. Allowed to root around the DNC unopposed, Cozy Bear could have harvested much of the material released during the 2016 campaign to embarrass Hillary Clinton and her key supporters within the party. One would expect U.S. intelligence to try to prevent that kind of thing.

One possible answer to that question has to do with timing. If the Dutch hackers only managed a year as flies on Cozy Bear's wall, they were out soon after discovering the DNC breach. That would suggest Crowdstrike and U.S. intelligence agencies were powerless to kick Cozy Bear off the DNC network without the Dutch help. On the other hand, if the Dutch held on for 2.5 years, that explanation doesn't work.

It also appears that the Dutch hackers didn't detect a second Russian intrusion into the DNC, by APT 28, or Fancy Bear, a group Crowdstrike links to GRU military intelligence: They didn't have access to this group's network.

The other important question that arises from the Dutch story is, if the U.S. had specific evidence of the breach and earlier APT 29 efforts, as well as pictures from the security camera at the group's «office,» why aren't there any indictments of Russian officials and hackers. The evidence goes back more than three years, and the Dutch intelligence service has long since lost its access, meaning that Cozy Bear figured out it was being watched and, presumably, by what means. There's no longer any reason to protect those sources.

Last November, The Wall Street Journal reported, citing anonymous sources, that the Justice Department had identified «more than six members of the Russian government» involved in the DNC hack but that discussions about the case were «in the early stages.» That's difficult to understand if the evidence has been there since 2015.

My Bloomberg View colleague Eli Lake recently made a strong case for the release of all the classified memos that allegedly shed light on the Russian interference investigations. The secrecy around it is, indeed, excessive. The public deserves to know exactly how Russia meddled in the 2016 presidential election.

Specific evidence linking Russian intelligence to the DNC hack would dramatically change the current picture of limited attempts at interference via Facebook and the state-owned network Russia Today, especially if it could also be shown that material obtained in that Russian hack surfaced on Wikileaks. It serves no purpose to keep that kind of information from the public.

Leonid Bershidsky is a Bloomberg View columnist. He was the founding editor of the Russian business daily Vedomosti and founded the opinion website Slon.ru. The views and opinions expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2018/01/26/release-the-dutch-evidence-of-the-dnc-hack-a60300