GlobalResearch
Center for Research on Globalization

U.S. States: We Weren't Hacked by Russians in 2016

Shocker: the media ignores the fact there is no real evidence of election systems tampering.

By Gareth Porter
Global Research, August 19, 2019
The American Conservative 16 August 2019

Region: Russia and FSU, USA
Theme: Intelligence, Media Disinformation
In-depth Report: U.S. Elections

A "bombshell" Senate Intelligence Committee report released in July repeated the familiar claim that Russia targeted the electoral websites of at least 21 states—but statements from the states themselves effectively undermine that narrative.

It turns out the reality is dramatically different from the headlines.

The states' own summary responses contained in the report show that, with one exception, they found either no effort to penetrate any of their election-related sites or merely found scanning and probing associated with an IP address that the FBI had warned about ahead of the 2016 election. Hardly a slam dunk.

Federal authorities, including Independent Counsel Robert Mueller, later claimed that the Russians used that IP address to hack into the Illinois state election systems and access some 200,000 voter records, though Mueller provided no additional evidence for that in his report. Nor was there any evidence that any data was tampered with, or a single vote changed.

About the same time, in August 2016, it was reported that Arizona state election systems were also breached, and it was widely speculated afterward that the Russians were behind it. But the Senate committee itself acknowledged that it was a criminal matter, and didn't involve the Russians.

The "Russian" hack on the Illinois website, however, eventually became part of conventional wisdom, mainly because of Special Counsel Robert Mueller's indictment of 12 GRU (Russia's foreign intelligence agency) officers for allegedly carrying it out.

But the overarching reality here is that there was no real penetration anywhere else. As for outside "probing" and "testing of vulnerabilities" (which, when closely read, makes up the vast majority of the "targeting" cited in the Senate report), that is something that states contend with every day at the hands of an untold number of potential hackers, including, but not limited to, foreign actors.

As Lisa Vasa, Oregon's chief information security officer, explained to *The Washington Post*, the state blocks "upwards of 14 million attempts to access our network every day." And Colorado Secretary of State Wayne Williams told the *Post*that the kind of scanning that was discussed by DHS "happens hundreds, if not thousands, of times per day."

Furthermore, not all federal officials buy into the theory that the Illinois intrusion was

political—rather than criminal—in nature. In fact, DHS Assistant Secretary for Cyber Security and Communications Andy Ozment testified in late September 2016 that the aim of the hackers in the Illinois case was "possibly for the purpose of selling personal information," since they had stolen the data but made no effort to alter it online.

The Senate Intelligence Committee, DHS, and the intelligence community nevertheless chose to omit that reality from consideration, presumably because it would have interfered with their desired conclusion regarding the Russian cyber attacks on the 2016 election.

How the states refute DHS claims

The report says,

> "Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. election."

None of the 21 states in question except for Illinois are identified by the heavily redacted report. Instead they are identified by number (State 1, State 2, etc.), which the Committee explains was at the request of DHS and "some states." Their responses to the Committee's query on what they experienced in 2016 are summarized in a single sentence and expounded on at greater length in the report.

Six of those states told the Committee that they had seen no cyber threat whatsoever to their government websites. Thirteen reported some level of "probing or scanning" (one lasting all of one second) that involved one of the cyber tools or IP addresses that DHS/FBI viewed as possibly Russia-related (but otherwise there is no concrete evidence that the activity was related to election tampering).

Arizona ("State 4," based on the widely reported circumstances of the case) also contradicted the DHS position. The report acknowledges that there were two "rounds of cyber activity" on Arizona systems. But one was a successful phishing attack that was later attributed to criminals, not Russians.

> In the second, the DHS account states, "Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library." (The spokesman for the Arizona Secretary of State, Michele Regan, told this writer that DHS had admitted only under grilling by state officials that the only thing "targeted" ahead of the 2016 election had been the Phoenix Public Library.) However, the report admits that DHS "has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections."

Nevertheless DHS continues to include Arizona—along with the six other states that clearly rejected the DHS claims, and the rest that merely acknowledge evidence of scanning or probing—as being among the 21 states victimized by Russia.

Were cyber tools real evidence of Russia's role?

The role of those cyber tools and IP addresses underlines the political nature of the DHS position. The FBI had sent a "FLASH" message to state election officials on August 18, 2016 alerting them to the use of Acunetix and SQLMAP technologies and eight IP addresses during the successful hack into the Illinois state voter registration website. Although the FBI did not suggest that these were indicators of Russian involvement, they and DHS began treating them as such.

In fact, however, Acunetix is a commonly available and widely used tool for identifying website vulnerabilities, and SQLMAP is a widely used "open source" technology for detecting and exploiting database vulnerabilities.

Thus DHS was pushing the use of these tools as indicators of Russian hacking, even though such technology is common to virtually all criminal hackers.

DHS and FBI had linked the eight IP addresses with Russia, because six of the eight were traced to King Servers, a hosting service owned by a young Russian living in Siberia, and one had briefly hosted a Russian criminal market during 2015. But the fact that the web hosting service was Russian-owned doesn't necessarily mean that his clients were Russian government-related, and IP addresses change hands frequently.

The owner of the six IP addresses, Vladimir Fomenko, told the *New York Times* that he could provide specific data on the IP address used in the Illinois intrusion that could help the FBI investigation. The FBI, whose counterinsurgency branch was providing input to Mueller's Russia investigation, might have been expected to follow up on that lead. But Fomenko told me in a July 24, 2018 email that the FBI still had made no effort to contact him.

Lastly the Senate report itself seems to leave some question about whether these IP addresses and hacking tools were a solid indication of Russian election tampering.

> "IP addresses associated with the August 18, FLASH," the report says, "provided some indications the activity might be attributable to the Russian government, particularly the GRU [emphasis added]."

States haven't been quiet about how DHS is misreporting this story. After Wisconsin election officials protested the claim in September 2017 that its election website had been targeted, DHS was forced to acknowledge that it had in fact been another non-election state website that had been scanned. The same happened in California.

Contrary to every mainstream media story about it, the Senate Committee report actually shows that DHS created a spectacular story without any solid evidence to back it up. The Committee should have been investigating the misleading political tactics of DHS, instead of being a cheerleader for it.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Gareth Porter is an investigative reporter and regular contributor to The American

Conservative. He is also the author of Manufactured Crisis: The Untold Story of the Iran Nuclear Scare.
