GlobalResearch
Center for Research on Globalization

Dark Web Voter Database Report Casts New Doubts on Russian Election Hack Narrative

By Gareth Porter

Global Research, September 15, 2020
The Grayzone 13 September 2020

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

A new report showing that US state-level voter databases were publicly available calls into question the narrative that Russian intelligence "targeted" US state election-related websites in 2016.

***

A September 1 report in the Moscow daily *Kommersant* on a "dark web" site offering a database of personal information on millions of registered American voters undermines one of the central themes of the Russia hysteria pervading US politics.

Democratic politicians and corporate media pundits have long accepted it as fact that Russian intelligence "targeted" US state election-related websites in 2016. But the Kommersant report shows that those state registered voter databases were already available to anyone in the public domain, eliminating any official Russian motive for hacking state websites.

Kommersant reported that a user on a dark web Forum known as Gorka9 offered free access to databases containing the information of 7.6 million Michigan voters, along with the state voter databases of Connecticut, Arkansas, Florida and North Carolina.

There are differences between the Michigan database described by Gorka9 and the one that the State of Michigan releases to the public upon request. Tracy Wimmer, the spokesperson for the Michigan Secretary of State, said in an e-mail to Grayzone that when the Michigan voter registration database is released to the public upon request, the state withholds "date of birth (year of birth is included), driver's license number, the last four digitals of someone's social security number, email address and phone number…." However, Gorka9's description of the Michigan data includes driver's license numbers, full dates of birth, social security numbers and emails.

In fact both un-redacted and redacted state voter files are obviously widely available on the dark web as well as elsewhere on the internet. *Meduza,* a Russian-language news site based in Riga, Latvia, published the *Kommersant*story along with an "anonFiles" download portal for access to the Michigan voter database and a page from it showing that it is the officially redacted version. The DHS and the FBI both acknowledged in response to the Kommersant story that "a lot of voter registration data is publicly available or easily purchased."

> Joint Statement from #CISAgov and the @FBI on U.S. Elections #Protect2020
> pic.twitter.com/TcMBznikhz

> — Cybersecurity and Infrastructure Security Agency (@CISAgov) September 1, 2020

Criminal hackers have been seeking to extract such personal information from online state personal databases for many years — not only from voter registration databases but from drivers license, health care and other databases. Oregon's chief information security officer, **Lisa Vasa**, told the Washington Post in September 2017 that her team blocks "upwards of 14 million attempts to access our network every day."

Ken Menzell, the legal counsel to the Illinois state Board of Elections, told this writer in a 2017 interview that the only thing new about the hack of the state's voter database in 2016, in which personal data on 200,000 Illinois registered voters was exfiltrated, was that the hackers succeeded. Menzell recalled that hackers had been "trying constantly" to get into every Illinois personal database ever since 2006.

The motive for the hackers was simple: as observed by Andrey Arsentiev, the head of analytics and special projects at the private security partnership, Infowatch, databases can be mined for profits on the dark web, primarily by selling them to scam artists working on a mass scale. Gorka9 was offering state voter files for free because the owner had already squeezed all the potential profit out of selling them.

For the Russian government, on the other hand, such databases would be of little or no value. When FBI counterintelligence chief **Bill Priestap** was asked by a member of the Senate Intelligence Committee in June 2017 how Moscow might use personal voter registration data, the only explanation he could come up with was that the Russian government and its intelligence agencies were completely ignorant of the character of U.S. state voter databases. "They took the data to understand what it consisted of," Priestap declared.

Priestap was obviously unaware of the absurdity of the suggestion that the Russian government had no idea what was in such databases in 2016. After all, the state voter registration databases had already been released by the states themselves into the public domain, and had been bought and sold on the dark web for many years. The FBI has steered clear of the embarrassing suggestion by Priestap ever since.

Priestap's inability to conjure up a plausible reason for Russia to hack U.S. election sites points to the illogical and baseless nature of the claims of a Russian threat to the U.S. presidential election.

DHS creates the Russian cyber campaign against state election sites

Back in 2016, the Department of Homeland Security did its best to market the narrative of Russian infiltration of American voting systems. At the time, the DHS was seeking to increase its bureaucratic power by adding election infrastructure to its portfolio of cybersecurity responsibilities, and exploiting the Russian factor was just the ticket to supercharge their campaign.

In their prepared statement to the Senate Intelligence Committee in June 2017, two senior DHS officials, **Samuel Liles and Jeanette Manfra**, referred to an October 2016 intelligence report published by the DHS Office of Intelligence and Analysis. They stated it had “established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors.” That “potentially targeted” language gave away the fact that DHS didn’t have anything more than suspicion to back up the charge.

In fact DHS was unable to attribute any attempted election site hack to the Russian government. On October 7, 2016, in fact, DHS Secretary **Jeh Johnson** and Director of National Intelligence **James Clapper** stated explicitly that they could not do so. Liles and Manfra appeared to imply such an attribution, however, by associating DHS with a joint assessment by CIA, FBI and NSA released January 7, 2017, that contained the statement, the “Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards.”

But the meaning of that language was deliberately vague, and the only additional sentence related to it stated, “Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment.” That was far from any finding that Russia had scanned or hacked election-related websites.

In September 2017, under pressure from governors, DHS finally notified state governments about the cyber incidents that it had included in its October 2016 intelligence report as examples of “potential” Russan targeting. Now, it abandoned its ambiguous language and explicitly claimed Russian responsibility.

One state election official who asked not to be identified told this writer in a 2018 interview that “a couple of guys from DHS reading from a script” had informed him that his state was “targeted by Russian government cyber actors.”

DHS spokesman **Scott McConnell** issued a statement on September 28, 2017 that DHS “stood by” its assessment that 21 states “were the target of Russian government cyber actors seeking vulnerabilities and access to U.S. election infrastructure.” But McConnell also revealed that DHS had defined “targeting” so broadly that any public website that a hacker scanned in a state could be included within that definition.

The dishonest tactics the DHS employed to demonstrate plausible evidence of “targeting” was revealed by Arizona Secretary of State Michelle Reagan’s spokesperson **Matt Roberts**, who told this writer in an interview, “When we pressed DHS on what exactly was targeted, they said it was the Phoenix public library’s computer system.” Another 2016 hacking episode in Arizona, which the FBI originally believed was a Russian government job, was later found to be a common criminal hack. In that episode, a hacker had targeted a local official with a phishing scheme and managed to steal their username and password.

Ironically, DHS had speculated in its initial intelligence report that “that cyber operations targeting election infrastructure could be intended or used to undermine public confidence in electoral processes and potentially the outcome.”

That speculation, reiterated by corporate media, became a central feature of the Russiagate hysteria that electrified the Democratic Party’s base. None of the journalists and politicians who repeated the narrative stopped to consider how unsubstantiated claims by the DHS about Russian penetration of the US election infrastructure was doing just that – lowering public confidence in the democratic process.

The hysteria surrounding the supposed Russian threat to elections is far from over. The Senate Intelligence Committee report released in July 2019 sought to legitimize the contention by former Obama cyber security adviser **Michael Daniel** that Russia "may have" targeted all fifty states for cyber attacks on election-related sites. In explaining his reasoning to the Senate committee's staff, Daniel said: "My professional judgment was we have to work on the assumption [Russians] tried to go everywhere, because they're thorough, they're competent, they're good."

The New York Times eagerly played up that subjective and highly ideological judgment in the lede of a story headlined, "Russia Targeted Election Systems in All 50 States, Report Finds.'

As for DHS, it appeared to acknowledge by implication in an October 11, 2018 assessment excerpted in the Senate Committee report that it could not distinguish between a state-sponsored hack and a criminal hack. This August, the senior cybersecurity adviser for the Cybersecurity and Infrastructure Security Agency (CISA), **Matthew Masterson**, said,

> "We are not and have not seen specific targeting of those election systems that has been attributable to nation-state actors at this time.... We do see regular scanning, regular probing of election infrastructure as a whole, what you'd expect to see as you run IT systems."

Despite these stunning admissions, DHS has faced no official accountability for deliberately slanting its intelligence assessment to implicate Russia for common criminal hacking activity. No matter how shoddy its origins and development have proven to be, the narrative remains too politically useful to be allowed to die.

*

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 independent investigative journalist who has covered national security policy since 2005 and was the recipient of Gellhorn Prize for Journalism in 2012. His most recent book is The CIA Insider's Guide to the Iran Crisis co-authored with John Kiriakou, just published in February.*

The original source of this article is The Grayzone

Articles by: **Gareth Porter**

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

For media inquiries: publications@globalresearch.ca