Foisting Blame for Cyber-hacking on Russia

Exclusive: Cyber-criminal efforts to hack into U.S. government databases are epidemic, but this ugly reality is now being exploited to foist blame on Russia and fuel the New Cold War hysteria, reports Gareth Porter.

By Gareth Porter

Recent hearings by the Senate and House Intelligence Committees reflected the rising tide of Russian-election-hacking hysteria and contributed further to it. Both Democrats and Republicans on the two committees appeared to share the alarmist assumptions about Russian hacking, and the officials who testified did nothing to discourage the politicians.

On June 21, Samuel Liles, acting director of the Intelligence and Analysis Office's Cyber Division at the Department of Homeland Security, and Jeanette Manfra, acting deputy under secretary for cyber-security and communications, provided the main story line for the day in testimony before the Senate committee – that efforts to hack into election databases had been found in 21 states.

Former DHS Secretary Jeh Johnson and FBI counter-intelligence chief Bill Priestap also endorsed the narrative of Russian government responsibility for the intrusions on voter registration databases.

But none of those who testified offered any evidence to support this suspicion nor were they pushed to do so. And beneath the seemingly unanimous embrace of that narrative lies a very different story.

The Department of Homeland Security (DHS) has a record of spreading false stories about alleged Russian hacking into U.S. infrastructure, such as the tale of a Russian intrusion into the Burlington, Vermont electrical utility in December 2016 that DHS later admitted was untrue. There was another bogus DHS story about Russia hacking into a Springfield, Illinois water pump in November 2011.

So, there's a pattern here. Plus, investigators, assessing the notion that Russia hacked into state electoral databases, rejected that suspicion as false months ago. Last September, Assistant Secretary of DHS for Cybersecurity Andy Ozment and state officials explained that the intrusions were not carried out by Russian intelligence but by criminal hackers seeking personal information to sell on the Internet.

Both Ozment and state officials responsible for the state databases revealed that those databases have been the object of attempted intrusions for years. The FBI provided information to at least one state official indicating that the culprits in the hacking of the state's voter registration database were cyber-criminals.

Illinois is the one state where hackers succeeded in breaking into a voter registration database last summer. The crucial fact about the Illinois hacking, however, was that the hackers extracted personal information on roughly 90,000 registered voters, and that none of the information was expunged or altered.

The Actions of Cybercriminals

That was an obvious clue to the motive behind the hack. Assistant DHS Secretary Ozment testified before the House Subcommittee on Information Technology on Sept. 28 (at 01:02.30 of the video) that the apparent interest of the hackers in copying the data suggested that the hacking was "possibly for the purpose of selling personal information."

Ozment 's testimony provides the only credible motive for the large number of states found to have experienced what the intelligence community has called "scanning and probing" of computers to gain access to their electoral databases: the personal information involved – even e-mail addresses – is commercially valuable to the cybercriminal underworld.

That same testimony also explains why so many more states reported evidence of attempts to hack their electoral databases last summer and fall. After hackers had gone after the Illinois and Arizona databases, Ozment said, DHS had provided assistance to many states in detecting attempts to hack their voter registration and other databases.

"Any time you more carefully monitor a system you're going to see more bad guys poking and prodding at it," he observed, "*because they're always poking and prodding.*" [Emphasis added]

State election officials have confirmed Ozment's observation. Ken Menzel, the general counsel for the Illinois Secretary of State, told this writer, "What's new about what happened last year is not that someone tried to get into our system but that they finally succeeded in getting in." Menzel said hackers "have been trying constantly to get into it since 2006."

And it's not just state voter registration databases that cybercriminals are after, according to Menzel. "Every governmental data base – driver's licenses, health care, you name it – has people trying to get into it," he said.

Arizona Secretary of State Michele Reagan told Mother Jones that her I.T. specialists had detected 193,000 distinct attempts to get into the state's website in September 2016 alone and 11,000 appeared to be trying to "do harm."

Reagan further revealed that she had learned from the FBI that hackers had gotten a user name and password for their electoral database, and that it was being sold on the "dark web" – an encrypted network used by cyber criminals to buy and sell their wares. In fact, she said, the FBI told her that the probe of Arizona's database was the work of a "known hacker" who had been closely monitored "frequently."

James Comey's Role

The sequence of events indicates that the main person behind the narrative of Russian hacking state election databases from the beginning was former FBI Director James Comey. In testimony to the House Judiciary Committee on Sept. 28, Comey suggested that the Russian government was behind efforts to penetrate voter databases, but never said so directly.

Comey told the committee that FBI Counterintelligence was working to "understand just what mischief Russia is up to with regard to our elections." Then he referred to "a variety of scanning activities" and "attempted intrusions" into election-related computers "beyond what we knew about in July and August," encouraging the inference that it had been done by Russian agents.

The media then suddenly found unnamed sources ready to accuse Russia of hacking election data even while admitting that they lacked evidence. The day after Comey's testimony ABC headlined, "Russia Hacking Targeted Nearly Half of States' Voter Registration Systems, Successfully Infiltrating 4." The story itself revealed, however, that it was merely a suspicion held by "knowledgeable" sources.

Similarly, NBC News headline announced, "Russians Hacked Two U.S. Voter Databases, Officials Say." But those who actually read the story closely learned that in fact none of the unnamed sources it cited were actually attributing the hacking to the Russians.

It didn't take long for Democrats to turn the Comey teaser – and these anonymously sourced stories with misleading headlines about Russian database hacking – into an established fact. A few days later, the ranking Democrat on the House Intelligence Committee, Rep. Adam Schiff declared that there was "no doubt" Russia was behind the hacks on state electoral databases.

On Oct. 7, DHS and the Office of the Director of National Intelligence issued a joint statement that they were "not in a position to attribute this activity to

the Russian government." But only a few weeks later, DHS participated with FBI in issuing a "Joint Analysis Report" on "Russian malicious cyber activity" that did not refer directly to scanning and spearphishing aimed of state electoral databases but attributed all hacks related to the election to "actors likely associated with RIS [Russian Intelligence Services]."

Suspect Claims

But that claim of a "likely" link between the hackers and Russia was not only speculative but highly suspect. The authors of the DHS-ODNI report claimed the link was "supported by technical indicators from the U.S. intelligence community, DHS, FBI, the private sector and other entities." They cited a list of hundreds of I.P. addresses and other such "indicators" used by hackers they called "Grizzly Steppe" who were supposedly linked to Russian intelligence.

But as I reported last January, the staff of Dragos Security, whose CEO Rob Lee, had been the architect of a U.S. government system for defense against cyber attack, pointed out that the vast majority of those indicators would certainly have produced "false positives."

Then, on Jan. 6 came the "intelligence community assessment" – produced by selected analysts from CIA, FBI and National Security Agency and devoted almost entirely to the hacking of e-mail of the Democratic National Committee and Hillary Clinton's campaign chairman John Podesta. But it included a statement that "Russian intelligence obtained and maintained access to elements of multiple state or local election boards." Still, no evidence was evinced on this alleged link between the hackers and Russian intelligence.

Over the following months, the narrative of hacked voter registration databases receded into the background as the drumbeat of media accounts about contacts between figures associated with the Trump campaign and Russians built to a crescendo, albeit without any actual evidence of collusion regarding the e-mail disclosures.

But a June 5 story brought the voter-data story back into the headlines. The story, published by The Intercept, accepted at face value an NSA report dated May 5, 2017, that asserted Russia's military intelligence agency, the GRU, had carried out a spear-phishing attack on a U.S. company providing election-related software and had sent e-mails with a malware-carrying word document to 122 addresses believed to be local government organizations.

But the highly classified NSA report made no reference to any evidence supporting such an attribution. The absence of any hint of signals intelligence supporting its conclusion makes it clear that the NSA report was based on

nothing more than the same kind of inconclusive “indicators” that had been used to establish the original narrative of Russians hacking electoral databases.

A Checkered History

So, the history of the U.S. government’s claim that Russian intelligence hacked into election databases reveals it to be a clear case of politically motivated analysis by the DHS and the Intelligence Community. Not only was the claim based on nothing more than inherently inconclusive technical indicators but no credible motive for Russian intelligence wanting personal information on registered voters was ever suggested.

Russian intelligence certainly has an interest in acquiring intelligence related to the likely outcome of American elections, but it would make no sense for Russia’s spies to acquire personal voting information about 90,000 registered voters in Illinois.

When FBI Counter-intelligence chief Priestap was asked at the June 21 hearing how Moscow might use such personal data, his tortured effort at an explanation clearly indicated that he was totally unprepared to answer the question.

“They took the data to understand what it consisted of,” said Priestap, “so they can affect better understanding and plan accordingly in regards to possibly impacting future election by knowing what is there and studying it.”

In contrast to that befuddled non-explanation, there is highly credible evidence that the FBI was well aware that the actual hackers in the cases of both Illinois and Arizona were motivated by the hope of personal gain.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. He is the author of the newly published *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare.*