How the Department of Homeland Security Created a Deceptive Tale of Russia Hacking US Voter Sites

The narrative about Russian cyberattacks on American election infrastructure is a self-interested abuse of power by DHS based on distortion of evidence, writes Gareth Porter.

By Gareth Porter
Special to Consortium News

The narrative of Russian intelligence attacking state and local election boards and threatening the integrity of U.S. elections has achieved near-universal acceptance by media and political elites. And now it has been accepted by the Trump administration's intelligence chief, Dan Coats, as well.

But the real story behind that narrative, recounted here for the first time, reveals that the Department of Homeland Security (DHS) created and nurtured an account that was grossly and deliberately deceptive.

DHS compiled an intelligence report suggesting hackers linked to the Russian government *could* have targeted voter-related websites in many states and then leaked a sensational story of Russian attacks on those sites without the qualifications that would have revealed a different story. When state election officials began asking questions, they discovered that the DHS claims were false and, in at least one case, laughable.

The National Security Agency and special counsel Robert Mueller's investigating team have also claimed evidence that Russian military intelligence was behind election infrastructure hacking, but on closer examination, those claims turn out to be speculative and misleading as well. Mueller's indictment of 12 GRU military intelligence officers does not cite any violations of U.S. election laws though it claims Russia interfered with the 2016 election.

A Sensational Story

On Sept. 29, 2016, a few weeks after the hacking of election-related websites in Illinois and Arizona, ABC News carried a sensational headline: “Russian Hackers Targeted Nearly Half of States’ Voter Registration Systems, Successfully Infiltrated 4.” The story itself reported that “more than 20 state election systems” had been hacked, and four states had been “breached” by hackers suspected of working for the Russian government. The story cited only sources “knowledgeable” about the matter, indicating that those who were pushing the story were eager to hide the institutional origins of the information.

Behind that sensational story was a federal agency seeking to establish its leadership within the national security state apparatus on cybersecurity, despite its limited resources for such responsibility. In late summer and fall 2016, the Department of Homeland Security was maneuvering politically to designate state and local voter registration databases and voting systems as “critical infrastructure.” Such a designation would make voter-related networks and websites under the protection a “priority sub-sector” in the DHS “National Infrastructure Protection Plan, which already included 16 such sub-sectors.

DHS Secretary Jeh Johnson and other senior DHS officials consulted with many state election officials in the hope of getting their approval for such a designation. Meanwhile, the DHS was finishing an intelligence report that would both highlight the Russian threat to U.S. election infrastructure and the role DHS could play in protecting it, thus creating political impetus to the designation. But several secretaries of state—the officials in charge of the election infrastructure in their state—strongly opposed the designation that Johnson wanted.

On Jan. 6, 2017—the same day three intelligence agencies released a joint “assessment” on Russian interference in the election—Johnson announced the designation anyway.

Media stories continued to reflect the official assumption that cyber attacks on state election websites were Russian-sponsored. Stunningly,

The Wall Street Journal reported in December 2016 that DHS was itself behind hacking attempts of Georgia's election database.

The facts surrounding the two actual breaches of state websites in Illinois and Arizona, as well as the broader context of cyberattacks on state websites, didn't support that premise at all.

In July, Illinois discovered an intrusion into its voter registration website and the theft of personal information on as many as 200,000 registered voters. (The 2018 Mueller indictments of GRU officers would unaccountably put the figure at 500,000.) Significantly, however, the hackers only had copied the information and had left it unchanged in the database.

That was a crucial clue to the motive behind the hack. DHS Assistant Secretary for Cyber Security and Communications Andy Ozment told a Congressional committee in late September 2016 that the fact hackers hadn't tampered with the voter data indicated that the aim of the theft was not to influence the electoral process. Instead, it was "possibly for the purpose of selling personal information." Ozment was contradicting the line that already was being taken on the Illinois and Arizona hacks by the National Protection and Programs Directorate and other senior DHS officials.

In an interview with me last year, Ken Menzel, the legal adviser to the Illinois secretary of state, confirmed what Ozment had testified. "Hackers have been trying constantly to get into it since 2006," Menzel said, adding that they had been probing every other official Illinois database with such personal data for vulnerabilities as well. "Every governmental database—driver's licenses, health care, you name it—has people trying to get into it," said Menzel.

In the other successful cyberattack on an electoral website, hackers had acquired the username and password for the voter database Arizona used during the summer, as Arizona Secretary of State Michele Reagan learned from the FBI. But the reason that it had become known, according to Reagan in an interview with Mother Jones, was that the login and password had shown up for sale on the dark web—the network of websites used by cyber criminals to sell stolen data and other

illicit wares.

Furthermore, the FBI had told her that the effort to penetrate the database was the work of a "known hacker" whom the FBI had monitored "frequently" in the past. Thus, there were reasons to believe that both Illinois and Arizona hacking incidents were linked to criminal hackers seeking information they could sell for profit.

Meanwhile, the FBI was unable to come up with any theory about what Russia might have intended to do with voter registration data such as what was taken in the Illinois hack. When FBI Counterintelligence official Bill Priestap was asked in a June 2017 hearing how Moscow might use such data, his answer revealed that he had no clue: "They took the data to understand what it consisted of," said the struggling Priestap, "so they can affect better understanding and plan accordingly in regards to possibly impacting future elections by knowing what is there and studying it."

The inability to think of any plausible way for the Russian government to use such data explains why DHS and the intelligence community adopted the argument, as senior DHS officials Samuel Liles and Jeanette Manfra put it, that the hacks "could be intended or used to undermine public confidence in electoral processes and potentially the outcome." But such a strategy could not have had any effect without a decision by DHS and the U.S. intelligence community to assert publicly that the intrusions and other scanning and probing were Russian operations, despite the absence of hard evidence. So DHS and other agencies were consciously sowing public doubts about U.S. elections that they were attributing to Russia.

DHS Reveals Its Self-Serving Methodology

In June 2017, Liles and Manfra testified to the Senate Intelligence Committee that an October 2016 DHS intelligence report had listed election systems in 21 states that were "potentially targeted by Russian government cyber actors." They revealed that the sensational story leaked to the press in late September 2016 had been based on a draft of the DHS report. And more importantly, their use of the phrase "potentially targeted" showed that they were arguing only that the

cyber incidents it listed were *possible* indications of a Russian attack on election infrastructure.

Furthermore, Liles and Manfra said the DHS report had "catalogued suspicious activity we observed on state government networks across the country," which had been "largely based on suspected malicious tactics and infrastructure." They were referring to a list of eight IP addresses an August 2016 FBI "flash alert" had obtained from the Illinois and Arizona intrusions, which DHS and FBI had not been able to attribute to the Russian government.

The DHS officials recalled that the DHS began to "receive reports of cyber-enabled scanning and probing of election-related infrastructure in some states, some of which appeared to originate from servers operated by a Russian company." Six of the eight IP addresses in the FBI alert were indeed traced to King Servers, owned by a young Russian living in Siberia. But as DHS cyber specialists knew well, the country of ownership of the server doesn't prove anything about who was responsible for hacking: As cybersecurity expert Jeffrey Carr pointed out, the Russian hackers who coordinated the Russian attack on Georgian government websites in 2008 used a Texas-based company as the hosting provider.

The cybersecurity firm ThreatConnect noted in 2016 that one of the other two IP addresses had hosted a Russian criminal market for five months in 2015. But that was not a serious indicator, either. Private IP addresses are reassigned frequently by server companies, so there is not a necessary connection between users of the same IP address at different times.

The DHS methodology of selecting reports of cyber incidents involving election-related websites as "potentially targeted" by Russian government-sponsored hackers was based on no objective evidence whatever. The resulting list appears to have included any one of the eight addresses as well as any attack or "scan" on a public website that could be linked in any way to elections.

This methodology conveniently ignored the fact that criminal hackers were constantly trying to get access to every database in those same

state, country and municipal systems. Not only for Illinois and Arizona officials, but state electoral officials.

In fact, 14 of the 21 states on the list experienced nothing more than the routine scanning that occurs every day, according to the Senate Intelligence Committee. Only six involved what was referred to as a "malicious access attempt," meaning an effort to penetrate the site. One of them was in Ohio, where the attempt to find a weakness lasted less than a second and was considered by DHS's internet security contractor a "non-event" at the time.

State Officials Force DHS to Tell the Truth

For a year, DHS did not inform the 21 states on its list that their election boards or other election-related sites had been attacked in a presumed Russian-sponsored operation. The excuse DHS officials cited was that it could not reveal such sensitive intelligence to state officials without security clearances. But the reluctance to reveal the details about each case was certainly related to the reasonable expectation that states would publicly challenge their claims, creating a potential serious embarrassment.

On Sept. 22, 2017, DHS notified 21 states about the cyber incidents that had been included in the October 2016 report. The public announcement of the notifications said DHS had notified each chief election officer of "any potential targeting we were aware of in their state leading up to the 2016 election." The phrase "potential targeting" again telegraphed the broad and vague criterion DHS had adopted, but it was ignored in media stories.

But the notifications, which took the form of phone calls lasting only a few minutes, provided a minimum of information and failed to convey the significant qualification that DHS was only suggesting targeting as a possibility. "It was a couple of guys from DHS reading from a script," recalled one state election official who asked not to be identified. "They said [our state] was targeted by Russian government cyber actors."

A number of state election officials recognized that this information

conflicted with what they knew. And if they complained, they got a more accurate picture from DHS. After Wisconsin Secretary of State Michael Haas demanded further clarification, he got an email response from a DHS official with a different account. "[B]ased on our external analysis," the official wrote, "the WI [Wisconsin] IP address affected belongs to the WI Department of Workforce Development, not the Elections Commission."

California Secretary of State Alex Padilla said DHS initially had notified his office "that Russian cyber actors 'scanned' California's Internet-facing systems in 2016, including Secretary of State websites." But under further questioning, DHS admitted to Padilla that what the hackers had targeted was the California Department of Technology's network.

Texas Secretary of State Rolando Pablos and Oklahoma Election Board spokesman Byron Dean also denied that any state website with voter- or election-related information had been targeted, and Pablos demanded that DHS "correct its erroneous notification."

Despite these embarrassing admissions, a statement issued by DHS spokesman Scott McConnell on Sept. 28, 2017 said the 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." The statement retreated from the previous admission that the notifications involved "potential targeting," but it also revealed for the first time that DHS had defined "targeting" very broadly indeed.

It said the category included "some cases" involving "direct scanning of targeted systems" but also cases in which "malicious actors scanned for vulnerabilities in networks that may be connected to those systems or have similar characteristics in order to gain information about how to later penetrate their target."

It is true that hackers may scan one website in the hope of learning something that could be useful for penetrating another website, as cybersecurity expert Prof. Herbert S. Lin of Stanford University explained to me in an interview. But including any incident in which

that motive was theoretical meant that any state website could be included on the DHS list, without any evidence it was related to a political motive.

Arizona's further exchanges with DHS revealed just how far DHS had gone in exploiting that escape clause in order to add more states to its "targeted" list. Arizona Secretary of State Michele Reagan tweeted that DHS had informed her that "the Russian government targeted our voter registration systems in 2016." After meeting with DHS officials in early October 2017, however, Reagan wrote in a blog post that DHS "could not confirm that any attempted Russian government hack occurred whatsoever to any election-related system in Arizona, much less the statewide voter registration database."

What the DHS said in that meeting, as Reagan's spokesman Matt Roberts recounted to me, is even more shocking. "When we pressed DHS on what exactly was actually targeted, they said it was the Phoenix public library's computers system," Roberts recalled.

In April 2018, a CBS News "60 Minutes" segment reported that the October 2016 DHS intelligence report had included the Russian government hacking of a "county database in Arizona." Responding to that CBS report, an unidentified "senior Trump administration official" who was well-briefed on the DHS report told Reuters that "media reports" on the issue had sometimes "conflated criminal hacking with Russian government activity," and that the cyberattack on the target in Arizona "was not perpetrated by the Russian government."

NSA Finds a GRU Election Plot

NSA intelligence analysts claimed in a May 2017 analysis to have documented an effort by Russian military intelligence (GRU) to hack into U.S. electoral institutions. In an intelligence analysis obtained by *The Intercept* and reported in June 2017, NSA analysts wrote that the GRU had sent a spear-phishing email—one with an attachment designed to look exactly like one from a trusted institution but that contains malware design to get control of the computer—to a vendor of voting machine technology in Florida. The hackers then designed a fake web page that looked like that of the vendor. They sent it to a list

of 122 email addresses NSA believed to be local government organizations that probably were "involved in the management of voter registration systems." The objective of the new spear-phishing campaign, the NSA suggested, was to get control of their computers through malware to carry out the exfiltration of voter-related data.

But the authors of *The Intercept* story failed to notice crucial details in the NSA report that should have tipped them off that the attribution of the spear-phishing campaign to the GRU was based merely on the analysts' own judgment—and that their judgment was faulty.

The Intercept article included a color-coded chart from the original NSA report that provides crucial information missing from the text of the NSA analysis itself as well as *The Intercept*'s account. The chart clearly distinguishes between the elements of the NSA's account of the alleged Russian scheme that were based on "Confirmed Information" (shown in green) and those that were based on "Analyst Judgment" (shown in yellow). The connection between the "operator" of the spear-phishing campaign the report describes and an unidentified entity confirmed to be under the authority of the GRU is shown as a yellow line, meaning that it is based on "Analyst Judgment" and labeled "probably."

A major criterion for any attribution of a hacking incident is whether there are strong similarities to previous hacks identified with a specific actor. But the chart concedes that "several characteristics" of the campaign depicted in the report distinguish it from "another major GRU spear-phishing program," the identity of which has been redacted from the report.

The NSA chart refers to evidence that the same operator also had launched spear-phishing campaigns on other web-based mail applications, including the Russian company "Mail.ru." Those targets suggest that the actors were more likely Russian criminal hackers rather than Russian military intelligence.

Even more damaging to its case, the NSA reports that the same operator who had sent the spear-phishing emails also had sent a test email to the "American Samoa Election Office." Criminal hackers could have been

interested in personal information from the database associated with that office. But the idea that Russian military intelligence was planning to hack the voter rolls in American Samoa, an unincorporated U.S. territory with 56,000 inhabitants who can't even vote in U.S. presidential elections, is plainly risible.

The Mueller Indictment's Sleight of Hand

The Mueller indictment of GRU officers released on July 13 appeared at first reading to offer new evidence of Russian government responsibility for the hacking of Illinois and other state voter-related websites. A close analysis of the relevant paragraphs, however, confirms the lack of any real intelligence supporting that claim.

Mueller accused two GRU officers of working with unidentified "co-conspirators" on those hacks. But the only alleged evidence linking the GRU to the operators in the hacking incidents is the claim that a GRU official named Anatoly Kovalev and "co-conspirators" deleted search history related to the preparation for the hack after the FBI issued its alert on the hacking identifying the IP address associated with it in August 2016.

A careful reading of the relevant paragraphs shows that the claim is spurious. The first sentence in Paragraph 71 says that both Kovalev and his "co-conspirators" researched domains used by U.S. state boards of elections and other entities "for website vulnerabilities." The second says Kovalev and "co-conspirators" had searched for "state political party email addresses, including filtered queries for email addresses listed on state Republican Party websites."

Searching for website vulnerabilities would be evidence of intent to hack them, of course, but searching Republican Party websites for email addresses is hardly evidence of any hacking plan. And Paragraph 74 states that Kovalev "deleted his search history"—not the search histories of any "co-conspirator"—thus revealing that there were no joint searches and suggesting that the subject Kovalev had searched was Republican Party emails. So any deletion by Kovalev of his search history after the FBI alert would not be evidence of his involvement

in the hacking of the Illinois election board website.

With this rhetorical misdirection unraveled, it becomes clear that the repetition in every paragraph of the section of the phrase “Kovalev and his co-conspirators” was aimed at giving the reader the impression the accusation is based on hard intelligence about possible collusion that doesn’t exist.

The Need for Critical Scrutiny of DHS Cyberattack Claims

The DHS campaign to establish its role as the protector of U.S. electoral institutions is not the only case in which that agency has used a devious means to sow fear of Russian cyberattacks. In December 2016, DHS and the FBI published a long list of IP addresses as indicators of possible Russian cyberattacks. But most of the addresses on the list had no connection with Russian intelligence, as former U.S. government cyber-warfare officer Rob Lee found on close examination.

When someone at the Burlington, Vt., Electric Company spotted one of those IP addresses on one of its computers, the company reported it to DHS. But instead of quietly investigating the address to verify that it was indeed an indicator of Russian intrusion, DHS immediately informed *The Washington Post.* The result was a sensational story that Russian hackers had penetrated the U.S. power grid. In fact, the IP address in question was merely Yahoo’s email server, as Rob Lee told me, and the computer had not even been connected to the power grid. The threat to the power grid was a tall tale created by a DHS official, which the Post had to embarrassingly retract.

Since May 2017, DHS, in partnership with the FBI, has begun an even more ambitious campaign to focus public attention on what it says are Russian “targeting” and “intrusions” into “major, high value assets that operate components of our Nation’s critical infrastructure”, including energy, nuclear, water, aviation and critical manufacturing sectors. Any evidence of such an intrusion must be taken seriously by the U.S. government and reported by news media. But in light of the DHS record on alleged threats to election infrastructure and the Burlington power grid, and its well-known ambition to assume

leadership over cyber protection, the public interest demands that the news media examine DHS claims about Russian cyber threats far more critically than they have up to now.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. His latest book is *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare*.

If you valued this original article, please consider making a donation to Consortium News so we can bring you more stories like this one.