Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known

by **Michael Riley** and **Jordan Robertson**
June 13, 2017, 5:00 AM EDT

- Attackers said to take measure of voting systems, databases
- A 'red phone' warning to the Kremlin from Obama White House

Russia's cyberattack on the U.S. electoral system before Donald Trump's election was far more widespread than has been publicly revealed, including incursions into voter databases and software systems in almost twice as many states as previously reported.

In Illinois, investigators found evidence that cyber intruders tried to delete or alter voter data. The hackers accessed software designed to be used by poll workers on Election Day, and in at least one state accessed a campaign finance database. Details of the wave of attacks, in the summer and fall of 2016, were provided by three people with direct knowledge of the U.S. investigation into the matter. In all, the Russian hackers hit systems in a total of 39 states, one of them said.

Russian hacking of the 2016 U.S. election extended to 39 states. Bloomberg's Jordan Robertson reports.
Source: Bloomberg

The scope and sophistication so concerned Obama administration officials that they took an unprecedented step -- complaining directly to Moscow over a modern-day "red phone." In October, two of the people said, the White House contacted the Kremlin on the back channel to offer

detailed documents of what it said was Russia's role in election meddling and to warn that the attacks risked setting off a broader conflict.

Unwinding the Twists, Turns in Trump-Russia Probe: QuickTake Q&A <https://www.bloomberg.com/politics/articles/2017-05-09/unwinding-the-twists-turns-in-trump-russia-probe-quicktake-q-a>

The new details, buttressed by a classified National Security Agency document recently disclosed by the Intercept, show the scope of alleged hacking that federal investigators are scrutinizing as they look into whether Trump campaign officials may have colluded in the efforts. But they also paint a worrisome picture for future elections: The newest portrayal of potentially deep vulnerabilities in the U.S.'s patchwork of voting technologies comes less than a week after former FBI Director James Comey warned Congress that Moscow isn't done meddling.

"They're coming after America," Comey told the Senate Intelligence Committee investigating Russian interference in the election. "They will be back."

A spokeswoman for the Federal Bureau of Investigation in Washington declined to comment on the agency's probe.

Kremlin Denials

Russian officials have publicly denied any role in cyber attacks connected to the U.S. elections, including a massive "spear phishing" effort <https://www.bloomberg.com/politics/articles/2016-06-18/hackers-targeting-clinton-aides-struck-across-political-system> that compromised Hillary Clinton's campaign and the Democratic National Committee, among hundreds of other groups. President Vladimir Putin said in recent comments to reporters that criminals inside the country could have been involved without having been sanctioned by the Russian government.

How to See If Russia Meddled With Your Vote

One of the mysteries about the 2016 presidential election is why Russian intelligence, after gaining access to state and local systems, didn't try to disrupt the vote. One possibility is that the American warning was effective. Another former senior U.S. official, who asked for anonymity to discuss the classified U.S. probe into pre-election hacking, said a more likely explanation is that several months of hacking failed to give the attackers the access they needed to master America's disparate voting systems spread across more than 7,000 local jurisdictions.

Such operations need not change votes to be effective. In fact, the Obama administration believed that the Russians were possibly preparing to delete voter registration information or slow vote tallying in order to undermine confidence in the election. That effort went far beyond the carefully timed release of private communications by individuals and parties.

One former senior U.S. official expressed concern that the Russians now have three years to build on their knowledge of U.S. voting systems before the next presidential election, and there is every reason to believe they will use what they have learned in future attacks.

Secure Channel

As the first test of a communication system designed to de-escalate cyber conflict between the two countries, the cyber "red phone" -- not a phone, in fact, but a secure messaging channel for sending urgent messages and documents -- didn't quite work as the White House had hoped. NBC News first reported <http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116> that use of the red phone by the White House last December.

The White House provided evidence gathered on Russia's hacking efforts and reasons why the U.S. considered it dangerously aggressive. Russia responded by asking for more information and providing assurances that it would look into the matter even as the hacking continued, according to the two people familiar with the response.

"Last year, as we detected intrusions into websites managed by election officials around the country, the administration worked relentlessly to protect our election infrastructure," said Eric Schultz, a spokesman for former President Barack Obama. "Given that our election systems are so decentralized, that effort meant working with Democratic and Republican election administrators from all across the country to bolster their cyber defenses."

Illinois Database

Illinois, which was among the states that gave the FBI and the Department of Homeland Security almost full access to investigate its systems, provides a window into the hackers' successes and failures.

In early July 2016, a contractor who works two or three days a week at the state board of elections detected unauthorized data leaving the network, according to Ken Menzel, general counsel for the Illinois board of elections. The hackers had gained access to the state's voter database, which contained information such as names, dates of birth, genders, driver's licenses and partial Social Security numbers on 15 million people, half of whom were active voters. As many as 90,000 records were ultimately compromised.

But even if the entire database had been deleted, it might not have affected the election, according to Menzel. Counties upload records to the state, not the other way around, and no data moves from the database back to the counties, which run the elections. The hackers had no way of knowing that when they attacked the state database, Menzel said.

The state does, however, process online voter registration applications that are sent to the counties for approval, Menzel said. When voters are added to the county rolls, that information is then sent back to the state and added to the central database. This process, which is common across states, does present an opportunity for attackers to manipulate records at their inception.

Patient Zero

Illinois became Patient Zero in the government's probe, eventually leading investigators to a hacking pandemic that touched four out of every five U.S. states.

Using evidence from the Illinois computer banks, federal agents were able to develop digital “signatures” -- among them, Internet Protocol addresses used by the attackers -- to spot the hackers at work.

The signatures were then sent through Homeland Security alerts and other means to every state. Thirty-seven states reported finding traces of the hackers in various systems, according to one of the people familiar with the probe. In two others -- Florida and California -- those traces were found in systems run by a private contractor managing critical election systems.

(An NSA document reportedly leaked by Reality Winner <https://www.bloomberg.com/politics/articles/2017-06-08/accused-leaker-is-indicted-for-disclosing-classified-report> , the 25-year-old government contract worker arrested last week, identifies the Florida contractor as VR Systems, which makes an electronic voter identification system used by poll workers.)

In Illinois, investigators also found evidence that the hackers tried but failed to alter or delete some information in the database, an attempt that wasn’t previously reported. That suggested more than a mere spying mission and potentially a test run for a disruptive attack, according to the people familiar with the continuing U.S. counterintelligence inquiry.

States’ Response

That idea would obsess the Obama White House throughout the summer and fall of 2016, outweighing worries over the DNC hack and private Democratic campaign emails given to Wikileaks and other outlets, according to one of the people familiar with those conversations. The Homeland Security Department dispatched special teams to help states strengthen their cyber defenses, and some states hired private security companies to augment those efforts.

In many states, the extent of the Russian infiltration remains unclear. The federal government had no direct authority over state election systems, and some states offered limited cooperation. When then-DHS Secretary Jeh Johnson said last August that the department wanted to declare the systems as national critical infrastructure -- a designation that gives the federal government broader powers to intervene -- Republicans balked. Only after the election did the two sides eventually reach a deal to make the designation.

Relations with Russia remain strained. The cyber red phone was announced in 2011 as a provision in the countries’ Nuclear Risk Reduction Centers to allow urgent communication to defuse a possible cyber conflict. In 2008, what started during the Cold War as a teletype messaging system became a secure system for transferring messages and documents over fiber-optic lines.

After the Obama administration transmitted its documents and Russia asked for more information, the hackers’ work continued. According to the leaked NSA document, hackers working for Russian military intelligence were trying to take over the computers of 122 local election officials just days before the Nov. 8 election.

For more on Russia's cyber attacks, check out the *Decrypted* podcast:

While some inside the Obama administration pressed at the time to make the full scope of the Russian activity public, the White House was ultimately unwilling to risk public confidence in the election’s integrity, people familiar with those discussions said.