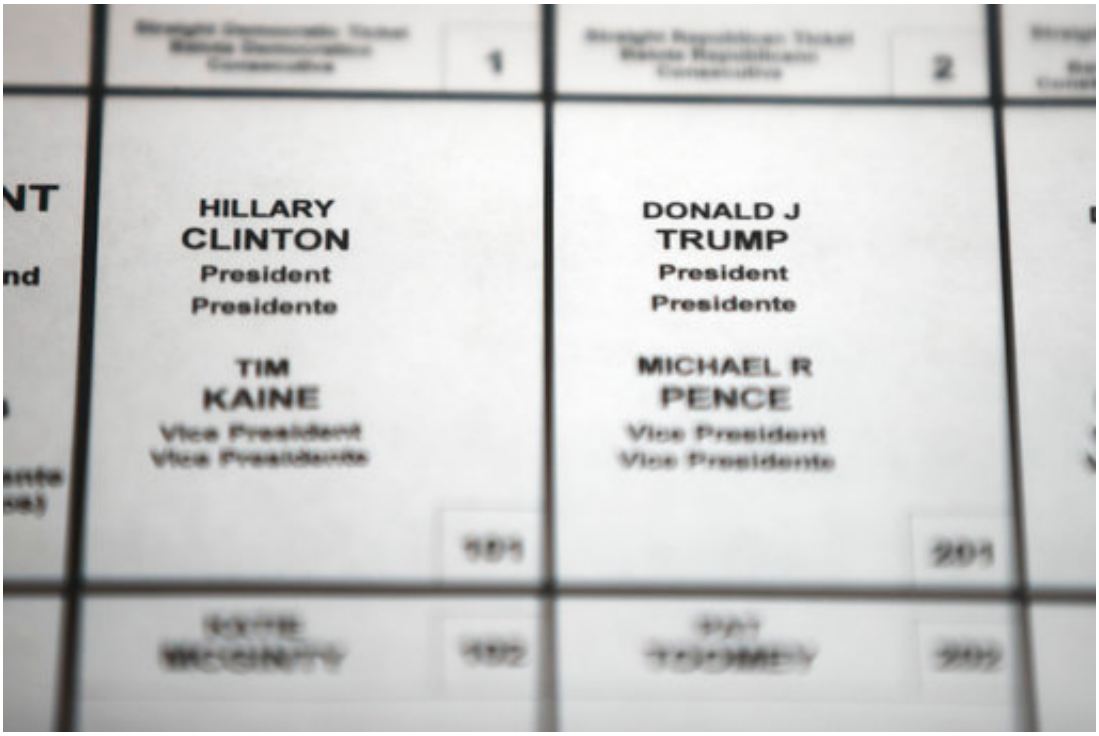
Alleged Russian hack reveals a deeply flawed election system

June 7 2017, by Frank Bajak



This Oct. 14, 2016 file photo shows Democratic presidential candidate Hillary Clinton's and Republican presidential candidate Donald Trump's names printed on a ballot on a voting machine to be used in the upcoming election, in Philadelphia. A newly leaked NSA document outlining alleged attempts by Russian military intelligence to hack into U.S. election systems is the latest piece of evidence suggesting a broad, sophisticated foreign attack on the integrity of U.S. elections. (AP Photo/Matt Rourke)

Election officials have long contended that the highly decentralized,

often ramshackle U.S. voting system is its own best defense against vote-rigging and sabotage . New evidence from a leaked intelligence report indicates that hasn't deterred foreign adversaries from exploring ways to attack it anyway.

The document, attributed to the U.S. National Security Agency, describes alleged attempts by Russian military intelligence to hack into local election systems—the latest evidence of a broad and sophisticated foreign attack on the integrity of U.S. elections. It does not indicate whether actual vote-tampering occurred.

The NSA report adds significant new detail to previous U.S. intelligence assessments that alleged Russia-backed hackers had compromised elements of America's electoral machinery. It also suggests that attackers may also have been laying groundwork for future subversive activity.

The U.S. elections system is a patchwork of more than 3,000 jurisdictions overseen by the states with almost no federal oversight or standards. The attack sketched out in the NSA document appears designed specifically to cope with that sprawl.

ELECTORAL RISK

The operation described in the document could have given attackers "a foothold into the IT systems of elections offices around the country that they could use to infect machines and launch a vote-stealing attack," said J. Alex Halderman, a University of Michigan computer scientist. "We don't have evidence that that happened," he said, "but that's a very real possibility."

Computer scientists have proven in the lab that once inside an election network, skillful attackers could manipulate pre-election programming of its systems and alter results without leaving a trace.

Sen. Mark Warner of Virginia, the ranking Democrat on the Senate intelligence committee, said Tuesday that hacking into state voting systems ahead of the Nov. 8 vote was more widespread than has been disclosed.

Attempts by Russia to "break into a number of our state voting processes" was "broad-based," he said, without offering details. In Moscow, a Kremlin spokesman categorically denied Tuesday that Moscow had tried to hack the U.S. elections.

Warner did not directly address the classified intelligence report published Monday by The Intercept, an online news outlet. The Associated Press has not independently verified the authenticity of the report, although its apparent leaker, an NSA contract worker, was arrested last weekend in Georgia.

GOING LOCAL

The NSA document says Russian military intelligence first targeted employees of a Florida voting systems supplier in August. Apparently exploiting technical data obtained in that operation, the cyber spies later sent phishing emails to 122 local U.S. election officials just days ahead of the Nov. 8 vote, intent on stealing their login credentials and breaking into the their systems, the document says.

The emails packed malware into Microsoft Word documents and were forged to give the appearance of being sent by the system vendor, VR Systems of Tallahassee, Florida.

The Department of Homeland Security knew in September that hackers believed to be Russian agents had targeted voter registration systems in more than 20 states. To date, no evidence of tampering with vote tallies or registration rolls has emerged.

The NSA document did not name any of the states where local officials were targeted by the emails masquerading as being from VR Systems. The Miami Herald reported Wednesday that officials in at least five Florida counties received the malicious emails described in the NSA report.

In September, the FBI held a conference call with all 67 county elections supervisors in that battleground state to inform them of infiltration of VR Systems without naming the company. Ion Sancho, who retired as Leon County supervisor in December, said he later learned from industry contacts that it was VR Systems.

LOCAL PROBLEMS

VR Systems officials did not respond directly to questions emailed by the AP. In a statement, the company said it only knows of a "handful" of customers who received the fraudulent email, adding that it had "no indication" that anyone had clicked on the malware. The NSA document says at least one account was likely compromised.

The company makes software for on-site voter registration at polling stations and backend systems for voting management, according to its website, which says it has customers in California, Florida, Illinois, Indiana, New York, North Carolina, Virginia, and West Virginia.

VR Systems' electronic poll books—electronic systems used to verify registered voters at polling places—experienced problems on Nov. 8 in Durham County, North Carolina. The issue forced officials to abandon the system, issue paper ballots and extend voting hours.

North Carolina's state elections director said Tuesday that officials would investigate to see if officials in Durham County were targeted and possibly compromised

Iowa University's Douglas Jones is among computer scientists who say voter registration systems are particularly vulnerable to tampering, in part because they are on the internet.

Someone trying to cause chaos and discredit an election could delete names from registration rolls prior to voting—or request absentee ballots en masse. In the latter case, a voter showing up at the polls on Election Day would be recorded as having already cast their ballot. That could force voters to file provisional ballots, and provoke long lines.

There is no evidence any of that happened last Election Day.