The New York Times | https://nyti.ms/2wXMSnS

POLITICS

Software Glitch or Russian Hackers? Election Problems Draw Little Scrutiny

By NICOLE PERLROTH, MICHAEL WINES and MATTHEW ROSENBERG SEPT. 1, 2017

The calls started flooding in from hundreds of irate North Carolina voters just after 7 a.m. on Election Day last November.

Dozens were told they were ineligible to vote and were turned away at the polls, even when they displayed current registration cards. Others were sent from one polling place to another, only to be rejected. Scores of voters were incorrectly told they had cast ballots days earlier. In one precinct, voting halted for two hours.

Susan Greenhalgh, a troubleshooter at a nonpartisan election monitoring group, was alarmed. Most of the complaints came from Durham, a blue-leaning county in a swing state. The problems involved electronic poll books — tablets and laptops, loaded with check-in software, that have increasingly replaced the thick binders of paper used to verify voters' identities and registration status. She knew that the company that provided Durham's software, VR Systems, had been penetrated by Russian hackers months before.

"It felt like tampering, or some kind of cyberattack," Ms. Greenhalgh said about the voting troubles in Durham.

There are plenty of other reasons for such breakdowns — local officials blamed human error and software malfunctions — and no clear-cut evidence of digital sabotage has emerged, much less a Russian role in it. Despite the disruptions, a record number of votes were cast in Durham, following a pattern there of overwhelming support for Democratic presidential candidates, this time Hillary Clinton.

But months later, for Ms. Greenhalgh, other election security experts and some state officials, questions still linger about what happened that day in Durham as well as other counties in North Carolina, Virginia, Georgia and Arizona.

After a presidential campaign scarred by Russian meddling, local, state and federal agencies have conducted little of the type of digital forensic investigation required to assess the impact, if any, on voting in at least 21 states whose election systems were targeted by Russian hackers, according to interviews with nearly two dozen national security and state officials and election technology specialists.

The assaults on the vast back-end election apparatus — voter-registration operations, state and local election databases, e-poll books and other equipment — have received far less attention than other aspects of the Russian interference, such as the hacking of Democratic emails and spreading of false or damaging information about Mrs. Clinton. Yet the hacking of electoral systems was more extensive than previously disclosed, The New York Times found.

Beyond VR Systems, hackers breached at least two other providers of critical election services well ahead of the 2016 voting, said current and former intelligence officials, speaking on condition of anonymity because the information is classified. The officials would not disclose the names of the companies.

Intelligence officials in January reassured Americans that there was no indication that Russian hackers had altered the vote count on Election Day, the bottom-line outcome. But the assurances stopped there.

Government officials said that they intentionally did not address the security of the back-end election systems, whose disruption could prevent voters from even casting ballots.

That's partly because states control elections; they have fewer resources than the federal government but have long been loath to allow even cursory federal intrusions into the voting process.

That, along with legal constraints on intelligence agencies' involvement in domestic issues, has hobbled any broad examination of Russian efforts to compromise American election systems. Those attempts include combing through voter databases, scanning for vulnerabilities or seeking to alter data, which have been identified in multiple states**.** Current congressional inquiries and the special counsel's Russia investigation have not focused on the matter.

"We don't know if any of the problems were an accident, or the random problems you get with computer systems, or whether it was a local hacker, or actual malfeasance by a sovereign nation-state," said Michael Daniel, who served as the cybersecurity coordinator in the Obama White House. "If you really want to know what happened, you'd have to do a lot of forensics, a lot of research and investigation, and you may not find out even then."

In interviews, academic and private election security experts acknowledged the challenges of such diagnostics but argued that the effort is necessary. They warned about what could come, perhaps as soon as next year's midterm elections, if the existing mix of outdated voting equipment, haphazard election-verification procedures and array of outside vendors is not improved to build an effective defense against Russian or other hackers.

In Durham, a local firm with limited digital forensics or software engineering expertise produced a confidential report, much of it involving interviews with poll workers, on the county's election problems. The report was obtained by The Times, and election technology specialists who reviewed it at the Times' request said the firm had not conducted any malware analysis or checked to see if any of the e-poll book software was altered, adding that the report produced more questions than answers.

Neither VR Systems — which operates in seven states beyond North Carolina — nor local officials were warned before Election Day that Russian hackers could have compromised their software. After problems arose, Durham County rebuffed help from the Department of Homeland Security and Free & Fair, a team of digital election-forensics experts who volunteered to conduct a free autopsy. The same was true elsewhere across the country.

"I always got stonewalled," said Joe Kiniry, the chief executive and chief scientist at Free & Fair.

Still, some of the incidents reported in North Carolina occur in every election, said Charles Stewart III, a political scientist at the Massachusetts Institute of Technology and an expert on election administration.

"Election officials and advocates and reporters who were watching most closely came away saying this was an amazingly quiet election," he said, playing down the notion of tampering. He added, though, that the problems in Durham and elsewhere raise questions about the auditing of e-poll books and security of small election vendors.

Ms. Greenhalgh shares those concerns. "We still don't know if Russian hackers did this," she said about what happened in North Carolina. "But we still don't know that they didn't."

Disorder at the Polls

North Carolina went for Donald J. Trump in a close election. But in Durham County, Hillary Clinton won 78 percent of the 156,000 votes, winning by a larger margin than President Barack Obama had against Mitt Romney four years earlier.

While only a fraction of voters were turned away because of the e-poll book difficulties — more than half of the county cast their ballots days earlier — plenty of others were affected when the state mandated that the entire county revert to paper rolls on Election Day. People steamed as everything slowed. Voters gave up and left polling places in droves — there's no way of knowing the numbers, but they include more than a hundred North Carolina Central University students facing four-hour delays.

At a call center operated by the monitoring group Election Protection, Ms. Greenhalgh was fielding technical complaints from voters in Mississippi, Texas and North Carolina. Only a handful came from the first two states.

Her account of the troubles matches complaints logged in the Election Incident Reporting System, a tracking tool created by nonprofit groups. As the problems mounted, The Charlotte Observer reported that Durham's e-poll book vendor was Florida-based VR Systems, which Ms. Greenhalgh knew from a CNN report had been hacked earlier by Russians. "Chills went through my spine," she recalled.

The vendor does not make the touch-screen equipment used to cast or tally votes and does not manage county data. But without the information needed to verify voters' identities and eligibility, which county officials load onto VR's poll books, voters cannot cast ballots at all.

Details of the breach did not emerge until June, in a classified National Security Agency report leaked to The Intercept, a national security news site. That report found that hackers from Russia's military intelligence agency, the G.R.U., had penetrated the company's computer systems as early as August 2016, then sent "spear-phishing" emails from a fake VR Systems account to 122 state and local election jurisdictions. The emails sought to trick election officials into downloading malicious software to take over their computers.

The N.S.A. analysis did not say whether the hackers had sabotaged voter data. "It is unknown," the agency concluded, whether Russian phishing "successfully compromised the intended victims, and what potential data could have been accessed."

VR Systems' chief operating officer, Ben Martin, said he did not believe Russian hackers were successful. He acknowledged that the vendor was a "juicy target," given that its systems are used in battleground states including North Carolina, Florida and Virginia. But he said that the company blocked access from its systems to local databases, and employs security protocols to bar intruders and digital triggers that sound alerts if its software is manipulated.

On Election Day, as the e-poll book problems continued, Ms. Greenhalgh urged an Election Protection colleague in North Carolina to warn the state Board of Elections of a cyberattack and suggest that it call in the F.B.I. and Department of Homeland Security. In an email, she also warned a Homeland Security election specialist of the problems. Later, the specialist told her Durham County had rejected the agency's help.

When Ms. Greenhalgh, who works at Verified Voting, a nonprofit dedicated to election integrity, followed up with the North Carolina colleague, he reported that state officials said they would not require federal help.

"He said: 'The state does not view this as a problem. There's nothing we can do, so we've moved on to other things,'" Ms. Greenhalgh recalled. "Meanwhile, I'm thinking, 'What could be more important to move on to?'"

An Interference Campaign

The idea of subverting the American vote by hacking election systems is not new. In an assessment of Russian cyberattacks released in January, intelligence agencies said Kremlin spy services had been collecting information on election processes, technology and equipment in the United States since early 2014.

The Russians shied away from measures that might alter the "tallying" of votes, the report added, a conclusion drawn from American spying and intercepts of Russian officials' communications and an analysis by the Department of Homeland Security, according to the current and former government officials.

The most obvious way to rig an election — controlling hundreds or thousands of decentralized voting machines — is also the most difficult. During a conference of computer hackers last month in Las Vegas, participants had direct access and quickly took over more than 30 voting machines. But remotely infiltrating machines of different makes and models and then covertly changing the vote count is far more challenging.

Beginning in 2015, the American officials said, Russian hackers focused instead on other internet-accessible targets: computers at the Democratic National

Committee, state and local voter databases, election websites, e-poll book vendors and other back-end election services.

Apart from the Russian influence campaign intended to undermine Mrs. Clinton and other Democratic officials, the impact of the quieter Russian hacking efforts at the state and county level has not been widely studied. Federal officials have been so tight-lipped that not even many election officials in the 21 states the hackers assaulted know whether their systems were compromised, in part because they have not been granted security clearances to examine the classified evidence.

The January intelligence assessment implied that the Russian hackers had achieved broader access than has been assumed. Without elaborating, the report said the Russians had "obtained and maintained access to multiple U.S. state and local election boards."

Two previously acknowledged strikes in June 2016 hint at Russian ambitions. In Arizona, Russian hackers successfully stole a username and password for an election official in Gila County. And in Illinois, Russian hackers inserted a malicious program into the Illinois State Board of Elections' database. According to Ken Menzel, the board's general counsel, the program tried unsuccessfully "to alter things other than voter data" — he declined to be more specific — and managed to illegally download registration files for 90,000 voters before being detected.

On Election Day last year, a number of counties reported problems similar to those in Durham. In North Carolina, e-poll book incidents occurred in the counties that are home to the state's largest cities, including Raleigh, Winston-Salem, Fayetteville and Charlotte. Three of Virginia's most populous counties — Prince William, Loudoun, and Henrico — as well as Fulton County, Georgia, which includes Atlanta, and Maricopa County, Arizona, which includes Phoenix, also reported difficulties. All were attributed to software glitches.

Senator Mark Warner, Democrat of Virginia and vice chairman of the Senate intelligence committee, argued for more scrutiny of suspicious incidents. "We must harden our cyber defenses, and thoroughly educate the American public about the danger posed" by attacks," he said in an email. "In other words: we are not making our elections any safer by withholding information about the scope and scale of the threat.”

In Durham County, officials have rejected any notion that an intruder sought to alter the election outcome. “We do not believe, and evidence does not suggest, that hacking occurred on Election Day,” Derek Bowens, the election director, said in a recent email.

But last month, after inquiries from reporters and the North Carolina State Board of Elections and Ethics Enforcement, Durham county officials voted to turn over laptops and other devices to the board for further analysis. It was not clear which government agency or private forensics firm, would conduct the investigation.

Ms. Greenhalgh will be watching closely. “What people focus on is, ‘Did someone mess with the vote totals?’” she said. “What they don’t realize is that messing with the e-poll books to keep people from voting is just as effective.’”

Follow Nicole Perlroth, Michael Wines, and Matthew Rosenberg on Twitter.