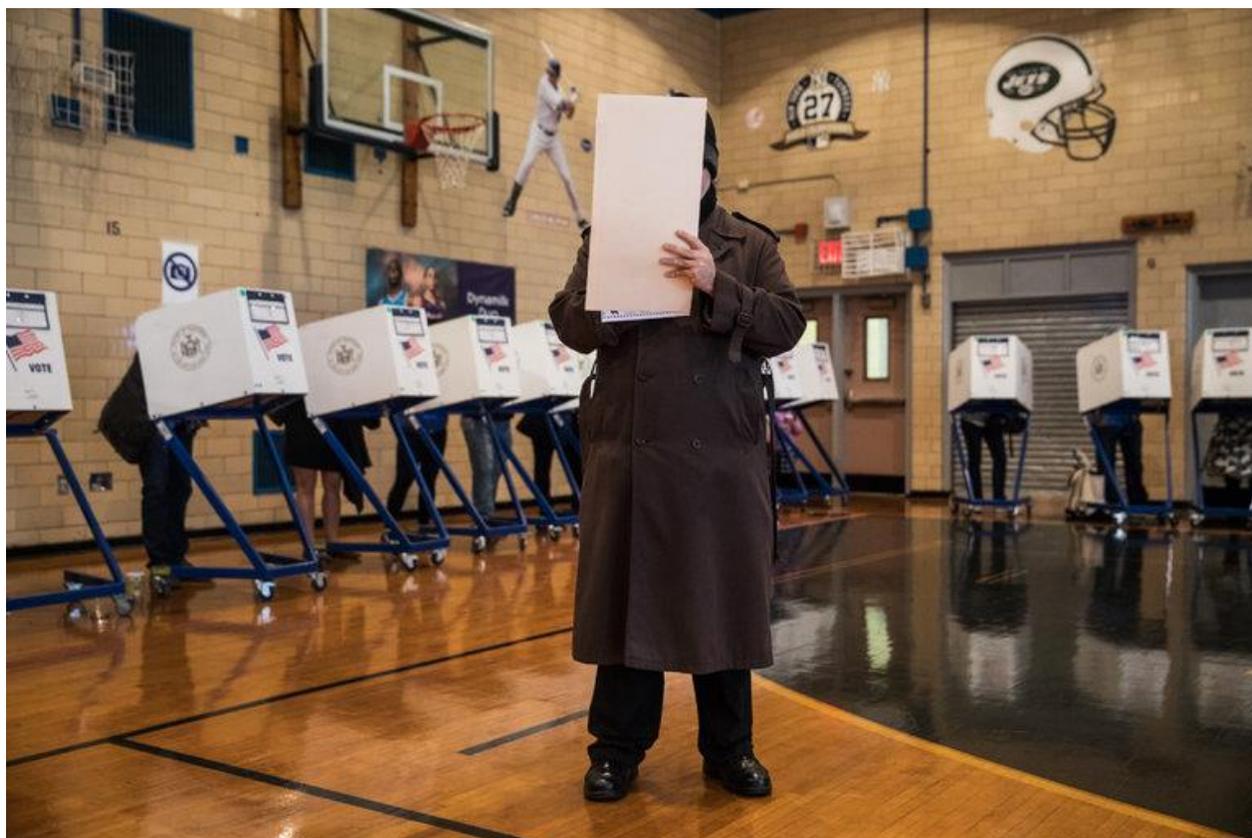


RUSSIAN INTERFERENCE IN THE 2016 U.S. PRESIDENTIAL ELECTION

In Election Interference, It's What Reporters Didn't Find That Matters

NICOLE PERLROTH, *The New York Times* Online Edition, September 1, 2017.



Voting at Public School 62 in Brooklyn in November. Credit: Todd Heisler/The New York Times

The story started, as many do, with our own confusion.

The most unusual of presidential elections — one marred by Russian trolls, a digital Watergate-style break-in and the winning candidate's dire warnings of a “rigged election” — was followed by the most unusual period of acceptance. In the immediate aftermath of the 2016 election, government officials, the Clinton campaign, intelligence analysts, and civic and legal groups all appeared to calmly accept claims that votes had not been hacked.

I had been on the cyber beat for six years and had grown accustomed to deep, often lengthy digital forensics analyses of cyberattacks against a wide range of targets: Silicon Valley start-ups, multinational conglomerates, government agencies and our own Times breach by Chinese government hackers. In the vast majority of cases, it takes investigators months or years to discover that hackers had indeed been lurking undetected on victims' machines.

Yet American intelligence officials were adamant in a report in January — just two months after Election Day — that vote tallies had not been hacked. This despite the broad consensus among United States intelligence agencies that Russia interfered in the 2016 election through an extensive disinformation and propaganda campaign, as well as the hacking of electoral databases and websites, the Democratic National Committee and the Democratic Congressional Campaign Committee.

My colleagues Michael Wines, Matthew Rosenberg and I set out to find out how government officials had nixed the possibility of vote hacking so readily. It was especially unclear to us given that officials at the Department of Homeland Security testified last fall that Russian hackers probed election systems in 21 states, with varying degrees of success, and that months later, a National Security Agency report found that Russian hackers had indeed successfully infiltrated VR Systems, an election service provider in eight states, including the battlegrounds North Carolina, Florida and Virginia.

As we dug more into [our investigation](#), the more unresolved incidents we found.

Among other things, we learned that intelligence agencies had intentionally worded their conclusions to specifically address “vote tallying,” not the back-end election systems — conclusions that were not even based on any in-depth investigation of the state election systems or the machines themselves, but on the accounts of American spies and digital intercepts of Russian communications, as well as on assessments by the Department of Homeland Security — which were largely superficial and not based on any in-depth investigation of the state election systems or machines themselves.

In fact, we discovered that precious little research had been conducted, the result of legal limits on the authority of intelligence agencies to address domestic issues and states’ historic reluctance to permit federal oversight of elections.

Michael Wines, who covers election issues for the Times, said that what stood out to him was the vulnerability of the nation’s vast Rube Goldberg election system. Elections, he explained, “are run by understaffed, underfinanced and sometimes undertrained local officials, serviced by outside contractors who may or may not be well vetted, conducted with equipment and software that may or may not be secure.”

And Matthew Rosenberg, who covers national security issues for the Times, discovered that the intelligence community’s conclusion — that the Election Day vote was not hacked — was extremely limited in scope.

I started calling around to the election security and technology experts who had witnessed some of the troubles that cropped up on Election Day. I found that they, too, were still searching for answers and were befuddled by the lack of any substantial investigation.

We zeroed in on Durham, N.C. — a reliably blue county in a swing state that went for Donald J. Trump — where a breakdown in the electronic check-in software prevented hundreds of would-be voters from casting their ballots and hundreds more to simply give up in the face of long lines.

Officials there relied on check-in software sold by VR Systems. Nobody in Durham — or any other county that relied on VR Systems’s electronic poll books — was ever informed that their equipment had been compromised by Russian hackers. And yet Durham

County officials rebuffed several offers to examine their systems at no cost — from the D.H.S., the F.B.I. and even Free & Fair, a group of qualified forensics investigators, many with security clearances.

Susan Greenhalgh, one of the few election technology specialists fielding technical complaints from North Carolina on Election Day, told me she was still haunted by what happened in November, and even more so by the lack of any follow-up investigation. “If you were looking to influence an election, one thing you could do is keep people from voting in a targeted county by monkeying with the e-pollbooks so people couldn’t check in, which would lead to long lines and chaos at the polls,” she said.

“This,” she told me, referring to what she witnessed in Durham on Election Day, “is exactly what that looked like.”

To this day, county, state, and federal officials have yet to investigate what transpired in Durham in November.

Instead, Durham officials asked Protus3, a little-known Raleigh firm comprised primarily of physical security experts and former law enforcement types with little, if any, of the technical expertise that is typically standard for breach investigations, to conduct an audit.

The firm’s confidential report was unlike any data breach investigation I have seen in my six years on this beat. Investigators had done none of the malware or coding forensics necessary to understand whether hackers had sabotaged VR Systems’s software, instead basing their analysis largely on eyewitness accounts of poll workers with limited technical understanding. When I shared the report with some of the top digital forensics experts in the country, many had visceral reactions: They simply could not believe that this was the definitive take on what transpired in Durham that day.

But through the course of our reporting, Michael, Matthew and I discovered that this was the norm.

There was a seeming lack of interest in doing much of anything about the problems on Election Day, or even in securing future elections. “Bills to tighten election security are languishing in congressional committees,” Michael noted. “The White House is focused on erasing fraud by individual voters, which experts say is a miniscule problem at its worst. A vast throng of voting machines that Congress financed after the disputed 2000 presidential election are now outdated, and no one wants to pony up the cash to modernize them.”

The more places we looked, the worse things looked. In fact, we discovered that VR Systems was not the only back-end supplier of election services that was hacked by Russians ahead of Election Day. Two more vendors that provide critical election services were also hacked.

Times Insider delivers behind-the-scenes insights from The New York Times. Visit us at [Times Insider](#) and follow us on [Twitter](#). Questions or feedback? [Email us](#).

A version of this article appears in print on September 2, 2017, on Page A2 of the New York edition with the headline: A Conspicuous Absence of Data.

Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny

NICOLE PERLROTH, MICHAEL WINES and MATTHEW ROSENBERG, *The New York Times* Online Edition, September 1, 2017.



A line outside a voting precinct before it opened on Election Day last year in Durham, N.C. Credit: Sara D. Davis/Getty Images

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.

Photo



Susan Greenhalgh, at her home in Amityville, N.Y. When she monitored complaints at an election call center last year, she was alarmed by disruptions reported in the swing state of North Carolina. Credit: An Rong Xu for The New York Times

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.



A man voting in Durham. Software that resulted in polling problems in the county was supplied by a company hacked by Russians months earlier. Credit Sara D. Davis/Getty Images

“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.”

A version of this article appears in print on September 2, 2017, on Page A1 of the New York edition with the headline: Little Effort to Investigate in States Targeted by Election Hacking.

Fake Russian Facebook Accounts Bought \$100,000 in Political Ads

SCOTT SHANE and VINDU GOEL, *The New York Times* National Edition, September 7, 2017, A1.



Facebook, already at the center of a storm over the role that it played in propagating misleading information during the presidential campaign, disclosed on Wednesday that fake accounts linked to Russia had purchased political ads on the social network last year. Credit: Jim Wilson/The New York Times

Providing new evidence of Russian interference in the 2016 election, Facebook disclosed on Wednesday that it had identified more than \$100,000 worth of divisive ads on hot-button issues purchased by a shadowy Russian company linked to the Kremlin.

Most of the 3,000 ads did not refer to particular candidates but instead focused on divisive social issues such as race, gay rights, gun control and immigration, according to a [post on Facebook](#) by Alex Stamos, the company's chief security officer. The ads, which ran between June 2015 and May 2017, were linked to some 470 fake accounts and pages the company said it had shut down.

Facebook officials said the fake accounts were created by a Russian company called [the Internet Research Agency](#), which is known for using "troll" accounts to post on social media and comment on news websites.

The disclosure adds to the evidence of the broad scope of the Russian influence campaign, which American intelligence agencies concluded was designed to damage

Hillary Clinton and boost Donald J. Trump during the election. Multiple investigations of the Russian meddling, and the possibility that the Trump campaign somehow colluded with Russia, have cast a shadow over the first eight months of Mr. Trump's presidency.

Facebook staff members on Wednesday briefed the Senate and House intelligence committees, which are investigating the Russian intervention in the American election. Mr. Stamos indicated that Facebook is also cooperating with investigators for Robert S. Mueller III, the special counsel, writing that “we have shared our findings with U.S. authorities investigating these issues, and we will continue to work with them as necessary.”

Mr. Stamos wrote that while some of the ads specifically mentioned the two candidates, most focused instead on issues that were polarizing the electorate: “divisive social and political messages across the ideological spectrum — touching on topics from LGBT matters to race issues to immigration to gun rights.”

Facebook did not make public any of the ads, nor did it say how many people saw them. But Mr. Trump regularly offered outspoken comments on those issues during the campaign, denouncing “political correctness” and rallying his supporters on the right.

Photo



Robert Mueller, the special counsel, is leading one of a number of investigations into Russia's role in last year's presidential election. Credit: Doug Mills/The New York Times

In its review of election-related advertising, Facebook said it had also found an additional 2,200 ads, costing \$50,000, that had less certain indications of a Russian connection. Some of those ads, for instance, were purchased by Facebook accounts with

internet protocol addresses that appeared to be in the United States but with the language set to Russian.

In a January report, the Federal Bureau of Investigation, Central Intelligence Agency and National Security Agency concluded that the Russian government, on direct orders from President Vladimir V. Putin, was responsible for hacking Democratic targets and leaking thousands of emails and other documents in an attempt to hurt Mrs. Clinton's campaign and mar her reputation.

The report also found that hundreds of Russian "trolls," or paid social media users, had posted anti-Clinton messages. But it did not name Facebook or address the question of advertising.

The January intelligence report said the "likely financier" of the Internet Research Agency was "a close Putin ally with ties to Russian intelligence." The company, [profiled by The New York Times Magazine](#) in 2015, is in St. Petersburg and uses its small army of trolls to put out messages supportive of Russian government policy.

The revelations can only add to the political skirmishing in Washington over Russia's role in the election. Mr. Trump has often dismissed the Russian hacking story as "fake news" and bristled at any implication that Mr. Putin had helped him win. To date, while news reports have uncovered many meetings and contacts between Trump associates and Russians, there has been no evidence proving collusion in the hacking or other Russian activities.

Representative Adam B. Schiff of California, the ranking Democrat on the House Intelligence Committee, said in a telephone interview that the Facebook disclosure "certainly quantifies the Russian use of at least one social media platform with a level of granularity that we did not have before." He said the committee has been in touch with Facebook for some time, adding, "I don't think this is the last word on the matter by Facebook or in terms of our investigation on the social media issue."

Mr. Schiff said he has more questions for Facebook, including when the company first become aware of the problem, what warning signs it found, how sophisticated the Russian operation was and what steps Facebook was taking to guard against such activity in the future.

"Clearly Facebook doesn't want to become the arbiter of what's true and what's not true," Mr. Schiff said. "But they do have a civil responsibility to do the best they can to inform their users of when they're being manipulated by a foreign actor."

The suspicion that Russia had a hand in placing Facebook ads was first mentioned in a [Time magazine article](#) in May, but Wednesday's announcement was the company's first acknowledgment of the problem.

Facebook, which offers a sophisticated level of targeting to advertisers, has been in the [center of a storm](#) over the role that it played in propagating false news reports and other misleading information during the campaign. The company acknowledged in April that fake accounts were a problem and said it accepted the intelligence agencies' findings on the matter, but it avoided naming Russia.

Mr. Stamos's post on Wednesday was more forthright, saying that the fake Facebook accounts connected to the ads "likely operated out of Russia."

After initially denying that fake news on the service had any influence on the election, Facebook's chief executive, Mark Zuckerberg, has gradually come around to the notion that the company must do more. Facebook has implemented a series of steps to combat fake content, including recruiting outside reviewers to check out and flag dubious articles.

But the new measures do not directly affect Facebook ads. Advertisers pay to have particular Facebook posts displayed high in the news feeds of whatever group of people is targeted.

The audience for an ad can be chosen using broad factors, such as middle-aged American men, or very specific ones, such as mothers who live in Minneapolis and like churches and the Minnesota Twins.

That ability to target is valuable to political campaigns, and the company actively reaches out to candidates around the world to teach them how to use Facebook to get their messages out, including through paid advertising.

One question underlying the investigation of possible collusion between the Trump campaign and Russia is whether Russia-sponsored operators would have needed any guidance from American political experts. Facebook said that some of the ads linked to Russian accounts had targeted particular geographic areas, which may raise questions about whether anyone had helped direct such targeting.

Under federal law, foreign governments, companies and citizens are prohibited from spending money to influence American elections. Facebook's disclosure could add an additional element to the possible crimes under investigation by Mr. Mueller.

Vindu Goel reported from San Francisco, and Scott Shane from Baltimore. Matt Rosenberg contributed reporting from Washington.

The Fake Americans Russia Created to Influence the Election

SCOTT SHANE, *The New York Times* Online Edition, September 7, 2017.



The Facebook European headquarters in Dublin last year. On Facebook and Twitter, Russian fingerprints are on hundreds or thousands of fake accounts that regularly posted anti-Clinton messages. Credit: Chris Ratcliffe/Bloomberg

Sometimes an international offensive begins with a few shots that draw little notice. So it was last year when Melvin Redick of Harrisburg, Pa., a friendly-looking American with a backward baseball cap and a young daughter, posted on [Facebook](#) a link to a brand-new website.

“These guys show hidden truth about [Hillary Clinton](#), George Soros and other leaders of the US,” he wrote on June 8, 2016. “Visit #DCLeaks website. It’s really interesting!”

Mr. Redick turned out to be a remarkably elusive character. No Melvin Redick appears in Pennsylvania records, and his photos seem to be borrowed from an unsuspecting Brazilian. But this fictional concoction has earned a small spot in history: The Redick posts that morning were among the first public signs of an unprecedented foreign intervention in American democracy.



A Facebook post, by someone claiming to be Melvin Redick, promoting a website linked to the Russian military intelligence agency G.R.U. Credit: The New York Times

The DCLeaks site had gone live a few days earlier, posting the first samples of material, stolen from prominent Americans by Russian hackers, that would reverberate through the presidential election campaign and into the Trump presidency. The site's phony promoters were in the vanguard of a cyberarmy of counterfeit Facebook and [Twitter](#) accounts, a legion of Russian-controlled impostors whose operations are still being unraveled.

The Russian information attack on the election did not stop with the hacking and leaking of Democratic emails or the fire hose of stories, true, false and in between, that battered Mrs. Clinton on Russian outlets like RT and Sputnik. Far less splashy, and far more difficult to trace, was Russia's experimentation on Facebook and Twitter, the American companies that essentially invented the tools of social media and, in this case, did not stop them from being turned into engines of deception and propaganda.

An investigation by The New York Times, and new research from the cybersecurity firm FireEye, reveals some of the mechanisms by which suspected Russian operators used Twitter and Facebook to spread anti-Clinton messages and promote the hacked material they had leaked. On Wednesday, [Facebook officials](#) disclosed that they had shut down several hundred accounts that they believe were created by a Russian company linked to the Kremlin and used to buy \$100,000 in ads pushing divisive issues during and after the American election campaign.

On Twitter, as on Facebook, Russian fingerprints are on hundreds or thousands of fake accounts that regularly posted anti-Clinton messages. Many were automated Twitter accounts, called bots, that sometimes fired off identical messages seconds apart — and in the exact alphabetical order of their made-up names, according to the FireEye researchers. On Election Day, for instance, they found that one group of Twitter bots sent out the hashtag #WarAgainstDemocrats more than 1,700 times.

The Russian efforts were sometimes crude or off-key, with a trial-and-error feel, and many of the suspect posts were not widely shared. The fakery may have added only modestly to the din of genuine American voices in the pre-election melee, but it helped fuel a fire of anger and suspicion in a polarized country.

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.



A Times investigation reveals missed signals, slow responses and a continuing underestimation of the seriousness of a campaign to disrupt the 2016 presidential election.

Given the powerful role of social media in political contests, understanding the Russian efforts will be crucial in preventing or blunting similar, or more sophisticated, attacks in the 2018 congressional races and the 2020 presidential election. Multiple government agencies have investigated the Russian attack, though it remains unclear whether any agency is focused specifically on tracking foreign intervention in social media. Both Facebook and Twitter say they are studying the 2016 experience and how to defend against such meddling.

“We know we have to stay vigilant to keep ahead of people who try to misuse our platform,” Alex Stamos, Facebook’s chief security officer, [wrote on Wednesday in a post](#) about the Russia-linked fake accounts and ads. “We believe in protecting the integrity of civic discourse.”

Critics say that because shareholders judge the companies partly based on a crucial data point — “monthly active users” — they are reluctant to police their sites too aggressively for fear of reducing that number. The companies use technical tools and teams of analysts to detect bogus accounts, but the scale of the sites — 328 million users on Twitter, nearly two billion on Facebook — means they often remove impostors only in response to complaints.

Though both companies have been slow to grapple with the problem of manipulation, they have stepped up efforts to purge fake accounts. Facebook says it takes down a million accounts a day — including some that were related to the recent French election and upcoming German voting — but struggles to keep up with the illicit activity. Still, the company says the abuse affects only a small fraction of the social network; Facebook officials [estimated](#) that of all the “civic content” posted on the site in connection with the United States election, less than one-tenth of one percent resulted from “information operations” like the Russian campaign.

Twitter, unlike Facebook, does not require the use of a real name and does not prohibit automated accounts, arguing that it seeks to be a forum for open debate. But it constantly updates a “trends” list of most-discussed topics or hashtags, and it says it tries to foil attempts to use bots to create fake trends. However, FireEye found that the suspected Russian bots sometimes managed to do just that, in one case causing the hashtag #HillaryDown to be listed as a trend.

Clinton Watts, a former F.B.I. agent who has closely tracked Russian activity online, said that Facebook and Twitter suffered from a “bot cancer eroding trust on their platforms.” But he added that while Facebook “has begun cutting out the tumors by deleting false accounts and fighting fake news,” Twitter has done little and as a result, “bots have only spread since the election.”

Asked to comment, Twitter referred to a blog post in June in which it said it was “doubling down” on efforts to prevent manipulation but could not reveal details for fear of tipping off those trying to evade the company’s measures. But it declared that Twitter’s “open and real-time nature is a powerful antidote” to falsehoods.

“This is important because we cannot distinguish whether every single Tweet from every person is truthful or not,” the statement said. “We, as a company, should not be the arbiter of truth.”

Leaks and Counterfeit Profiles

Russia has been quite open about playing its hacking card. In February last year, at a conference in Moscow, a top cyberintelligence adviser to President [Vladimir V. Putin](#) hinted that Russia was about to unleash a devastating information attack on the United States.

“We are living in 1948,” said the adviser, Andrey Krutskikh, referring to the eve of the first Soviet atomic bomb test, in [a speech](#) reported by The Washington Post. “I’m warning you: We are at the verge of having something in the information arena that will allow to us to talk to the Americans as equals.”

Mr. Putin’s denials of Russian meddling have been coy. [In June, he allowed](#) that “free-spirited” hackers might have awakened in a good mood one day and spontaneously decided to contribute to “the fight against those who say bad things about Russia.” [Speaking to NBC News](#), he rejected the idea that evidence pointed to Russia — while showing a striking familiarity with how cyberattackers might cover their tracks.

“IP addresses can be simply made up,” Mr. Putin said, referring to Internet protocol addresses, which can identify particular computers. “There are such IT specialists in the world today, and they can arrange anything and then blame it on whomever. This is no proof.”

Mr. Putin had a point. Especially in the social media realm, attributing fake accounts — to Russia or to any other source — is always challenging. [In January, the Central Intelligence Agency, the Federal Bureau of Investigation and the National Security Agency concluded](#) “with high confidence” that Mr. Putin had ordered an influence operation to damage Mrs. Clinton’s campaign and eventually aid [Donald J. Trump](#)’s. In April, Facebook published a [public report on information operations](#) using fake accounts. It shied away from naming Russia as the culprit until Wednesday, when the company said it had removed 470 “inauthentic” accounts and pages that were “likely operated out of Russia.” Facebook officials fingered a St. Petersburg company with Kremlin ties called [the Internet Research Agency](#).



President Vladimir V. Putin of Russia in June. His denials of Russian meddling have been coy, though he said that “free-spirited” hackers might have spontaneously contributed to “the fight against those who say bad things about Russia.” Credit: Sputnik, via Reuters

Russia deliberately blurs its role in influence operations, American intelligence officials say. Even skilled investigators often cannot be sure if a particular Facebook post or Twitter bot came from Russian intelligence employees, paid “trolls” in Eastern Europe or hackers from Russia’s vast criminal underground. A Russian site called buyaccs.com (“Buy Bulk Accounts at Best Prices”) offers for sale a huge array of pre-existing social media accounts, including on Facebook and Twitter; like wine, the older accounts cost more, because their history makes chicanery harder to spot.

The trail that leads from the Russian operation to the bogus Melvin Redick, however, is fairly clear. United States intelligence concluded that DCLeaks.com was created in June 2016 by the Russian military intelligence agency G.R.U. The site began publishing an eclectic collection of hacked emails, notably from George Soros, the financier and Democratic donor, as well as a former NATO commander and some Democratic and Republican staffers. Some of the website’s language — calling Mrs. Clinton “President of the Democratic Party” and referring to her “electional staff” — seemed to belie its pose as a forum run by American activists.

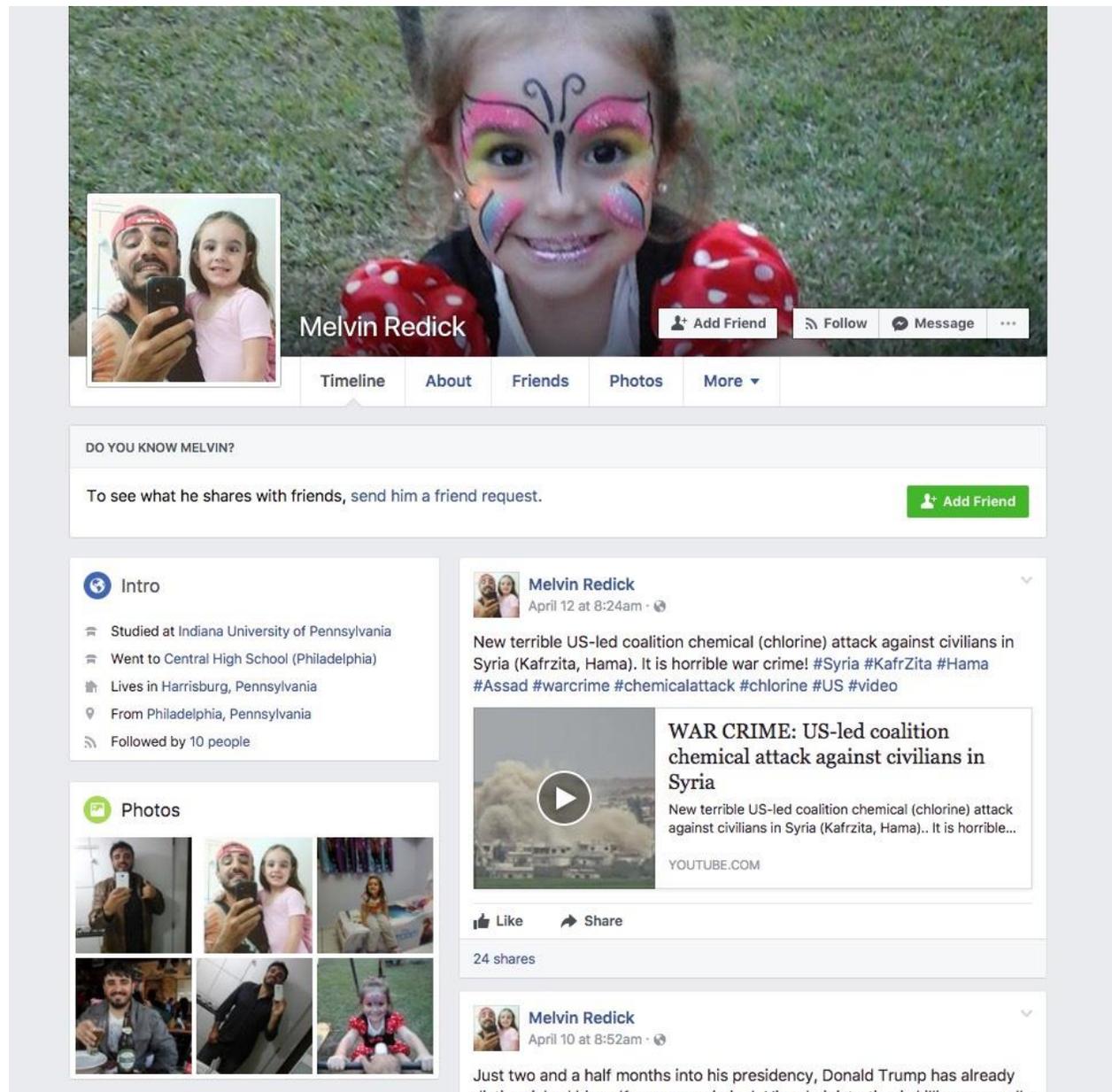
DCLeaks would soon be followed by a blog called Guccifer 2.0, which would leave even more clues of its Russian origin. Those sites’ posts, however, would then be dwarfed by those from WikiLeaks, which American officials believe got thousands of Democratic emails from Russian intelligence hackers through an intermediary. At each stage, a chorus of dubious Facebook and Twitter accounts — alongside many legitimate ones — would applaud the leaks.

During its first weeks online, DCLeaks drew no media attention. But The Times found that some Facebook users somehow discovered the new site quickly and began promoting it on June 8. One was the Redick account, which posted about DCLeaks to the Facebook groups “World News Headlines” and “Breaking News — World.”

The Redick profile lists Central High School in Philadelphia and Indiana University of Pennsylvania as his alma maters; neither has any record of his attendance. In one of his photos, this purported Pennsylvania lifer is sitting in a restaurant in Brazil — and in another, his daughter’s bedroom appears to have a Brazilian-style electrical outlet. His posts were never personal, just news articles reflecting a pro-Russian worldview.

Melvin Redick’s Facebook Profile

Inconsistencies in the contents of Mr. Redick’s Facebook profile suggest that the identity was fabricated.



1. Neither Central High School nor Indiana University of Pennsylvania has any record of Mr. Redick attending.
2. According to his profile, Mr. Redick was born and raised in Pennsylvania, but one image shows him seated in a restaurant in Brazil, and another shows a Brazilian-style electrical outlet in his daughter's bedroom.
3. Mr. Redick's posts were never of a personal nature. He shared only news articles reflecting a pro-Russian worldview.

The same morning, “Katherine Fulton” also began promoting DCLeaks in the same awkward English Mr. Redick used. “Hey truth seekers!” she wrote. “Who can tell me who are #DCLeaks? Some kind of Wikileaks? You should visit their website, it contains confidential information about our leaders such as Hillary Clinton, and others <http://dcleaks.com/>.”

So did “Alice Donovan,” who pointed to documents from Mr. Soros's Open Society Foundations that she said showed its pro-American tilt and — in rather formal language for Facebook — “describe eventual means and plans of supporting opposition movements, groups or individuals in various countries.”

Might Mr. Redick, Ms. Fulton, Ms. Donovan and others be real Americans who just happened to notice DCLeaks the same day? No. The Times asked Facebook about these and a half-dozen other accounts that appeared to be Russian creations. The company carried out its standard challenge procedure by asking the users to establish their bona fides. All the suspect accounts failed and were removed from Facebook.

Mobilizing a ‘Bot’ Army

On Twitter, meanwhile, hundreds of accounts were busy posting anti-Clinton messages and promoting the leaked material obtained by Russian hackers. Investigators for FireEye spent months reviewing Twitter accounts associated with certain online personas, posing as activists, that seemed to show the Russian hand: DCLeaks, Guccifer 2.0, Anonymous Poland and several others. FireEye concluded that they were associated with one another and with Russian hacking groups, including APT28 or Fancy Bear, which American intelligence blames for the hacking and leaking of Democratic emails.

Some accounts, the researchers found, showed clear signs of intermittent human control. But most displayed the rote behavior of automated Twitter bots, which send out tweets according to built-in instructions.

The researchers discovered long lists of bot accounts that sent out identical messages within seconds or minutes of one another, firing in alphabetical order. The researchers coined the term “warlist” for them. On Election Day, one such list cited leaks from Anonymous Poland in more than 1,700 tweets. Snippets of them provide a sample of the sequence:

@edanuro1 #WarAgainstDemocrats 17:54

@efekinoks #WarAgainstDemocrats 17:54

@elyashayk #WarAgainstDemocrats 17:54

@emreanbalc #WarAgainstDemocrats 17:55

@emrullahtac #WarAgainstDemocrats 17:55

Lee Foster, who leads the FireEye team examining information operations, said some of the warlist Twitter accounts had previously been used for illicit marketing, suggesting that they may have been purchased on the black market. Some were genuine accounts that had been hijacked. Rachel Usedom, a young American engineer in California, tweeted mostly about her sorority before losing interest in 2014. In November 2016, her account was taken over, [renamed #ClintonCorruption](#), and used to promote the Russian leaks.

Photo



Rachel Usedom’s Twitter account was taken over and used to post political leaks.

Ms. Usedom had no idea that her account had been commandeered by anti-Clinton propagandists. “I was shocked and slightly confused when I found out,” she said.

Notably, the warlist tweets often included the Twitter handles of users whose attention the senders wanted to catch — news organizations, journalists, government agencies and politicians, including @realDonaldTrump. By targeting such opinion-shapers, Mr. Foster said, the creators of the warlists clearly wanted to stir up conversation about the leaked material.

J. M. Berger, a researcher in Cambridge, Mass., helped build a [public web “dashboard”](#) for the Washington-based Alliance for Securing Democracy to track hundreds of Twitter accounts that were suspected of links to Russia or that spread Russian propaganda. During the campaign, he said, he often saw the accounts post replies to Mr. Trump’s tweets.

Mr. Trump “received more direct replies than anyone else,” Mr. Berger said. “Clearly this was an effort to influence Donald Trump. They know he reads tweets.”

The suspected Russian operators at times lacked sophistication. “They are not always Americanophiles who know every nuance of U.S. politics,” said Mr. Foster, the FireEye researcher.

For instance, last October, hundreds of Anonymous Poland Twitter accounts posted a forged letter on the stationery of the conservative Bradley Foundation, based in Milwaukee, purporting to show that it had donated \$150 million to the Clinton

campaign. The foundation denied any such contribution, which would have been illegal and, given its political leaning, highly unlikely.

‘A Battle of Information’

Only a small fraction of all the suspect social media accounts active during the election have been studied by investigators. But there is ample reason to suspect that the Russian meddling may have been far more widespread.

Several activists who ran Facebook pages for [Bernie Sanders](#), for instance, noticed a suspicious flood of hostile comments about Mrs. Clinton after Mr. Sanders had already ended his campaign and endorsed her.

John Mattes, who ran the “San Diego for Bernie Sanders” page, said he saw a shift from familiar local commenters to newcomers, some with Eastern European names — including four different accounts using the name “Oliver Mitov.”

“Those who voted for Bernie, will not vote for corrupt Hillary!” one of the Mitovs wrote on Oct. 7. “The Revolution must continue! #NeverHillary”

While he was concerned about being seen as a “crazy cold warrior,” Mr. Mattes said he came to believe that Russia was the likely source of the anti-Clinton comments. “The magnitude and viciousness of it — I would suggest that their fingerprints were on it and no one else had that agenda,” he said.

Both on the left and the pro-Trump right, though, some skeptics complain that Moscow has become the automatic boogeyman, accused of misdeeds with little proof. Even those who track Russian online activity admit that in the election it was not always easy to sort out who was who.

“Yes, the Russians were involved. Yes, there’s a lot of organic support for Trump,” said Andrew Weisburd, an Illinois online researcher who has written frequently about Russian influence on social media. “Trying to disaggregate the two was difficult, to put it mildly.”

Mr. Weisburd admitted that he had labeled some Twitter accounts “Kremlin trolls” based simply on their pro-Russia tweets and with no proof of Russian government ties. The Times contacted several such users, who insisted that they had come by their anti-American, pro-Russian views honestly, without payment or instructions from Moscow.

“Hillary’s a warmonger,” said Marilyn Justice, 66, who lives in Nova Scotia and tweets as [@mkj1951](#). Of Mr. Putin, she said in an interview, “I think he’s very patient in the face of provocations.”

Ms. Justice said she had first taken an interest in Russia during the 2014 Winter Olympics in Sochi, Russia, while looking for hockey coverage and finding what she considered a snide anti-Russia bias in the Western media. She said she did get a lot of news from Sputnik and RT but laughed at the notion that she could have Kremlin connections.

Another of the so-called Kremlin trolls, [Marcel Sardo](#), 48, a web producer in Zurich, describes himself bluntly on his Twitter bio as a “Pro-Russia Media-Sniper.” He said he

shared notes daily via Skype and Twitter with online acquaintances, including Ms. Justice, on disputes between Russia and the West over who shot down the Malaysian airliner hit by a missile over Ukraine and who used sarin gas in Syria.

“It’s a battle of information, and I and my peers have decided to take sides,” said Mr. Sardo, who constantly cites Russian sources and bashed Mrs. Clinton daily during the campaign. But he denied he had any links to the Russian government.

If that’s so, his prolific posts are a victory for Russia’s information war — that admirers of the Kremlin spread what American officials consider to be Russian disinformation on election hacking, Syria, Ukraine and more.

But if Russian officials are gleeful at their success, in last year’s election and beyond, they rarely let the mask slip. In [an interview with Bloomberg](#) before the election, Mr. Putin suggested that reporters were worrying too much about who exactly stole the material.

“Listen, does it even matter who hacked this data?” he said, in a point that Mr. Trump has sometimes echoed. “The important thing is the content that was given to the public.”

#####