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

'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020

By Matthew Rosenberg, Nicole Perlroth and David E. Sanger

Jan. 10, 2020

The National Security Agency and its British counterpart issued an unusual warning in October: The Russians were back and growing stealthier.

Groups linked to Russia's intelligence agencies, they noted, had recently been uncovered boring into the network of an elite Iranian hacking unit and attacking governments and private companies in the Middle East and Britain — hoping Tehran would be blamed for the havoc.

For federal and state officials charged with readying defenses for the 2020 election, it was a clear message that the next cyberwar was not going to be like the last. The landscape is evolving, and the piggybacking on Iranian networks was an example of what America's election-security officials and experts face as the United States enters what is shaping up to be an ugly campaign season marred by hacking and disinformation.

American defenses have vastly improved in the four years since Russian hackers and trolls mounted a broad campaign to sway the 2016 presidential election. Facebook is looking for threats it barely knew existed in 2016, such as fake ads paid for in rubles and self-proclaimed Texas secessionists logging in from St. Petersburg. Voting officials are learning about bots, ransomware and other vectors of digital mischief. Military officials are considering whether to embrace information warfare and retaliate against election interference by hacking senior Russian officials and leaking their personal emails or financial information.

Yet interviews with dozens of officials and experts make clear that many of the vulnerabilities exploited by Moscow in 2016 remain. Most political campaigns are unwilling to spend what it takes to set up effective cyberdefenses. Millions of Americans are still primed to swallow fake news. And those charged with protecting American elections face the same central challenge they did four years ago: to spot and head off any attack before it can disrupt voting or sow doubts about the outcome. It is a task made even more difficult by new threats to the election from other American rivals, such as Iran, which has more motive than ever to interfere in 2020 after a drone strike killed its top security and intelligence commander last week in Iraq.

The Russians were sloppy in 2016 because they could be: They caught Americans off guard. Now hackers and trolls, who have seen their tradecraft splashed across the pages of American intelligence assessments and federal indictments, are working far harder to cover their tracks. They are, as one American intelligence official put it, "refreshing" their operations.

One of the two Russian intelligence units that hacked the Democrats in 2016, known as "Fancy Bear," has shifted some of its work to servers based in the United States in an apparent attempt to thwart the N.S.A. and other American spy agencies, which are limited by law to operating abroad, according to federal officials tracking the moves. The other unit, known as "Cozy Bear," abandoned its hacking infrastructure six months ago and has dropped off the radar, security analysts said.

The trolls at the Internet Research Agency — the now-indicted outfit behind much of the Russian disinformation spread in 2016 — have ditched email accounts that were being tracked by Western intelligence agencies and moved to encrypted communication tools, like ProtonMail, that are much harder to trace. They are also trying to exploit a hole in Facebook's ban on foreigners buying political ads, paying American users to hand over personal pages and setting up offshore bank accounts to cover their financial tracks, said an official and a security expert at a prominent tech company.

At the Department of Homeland Security, there is renewed anxiety about a spate of ransomware attacks on American towns and cities over the last year. The attacks, officials say, revealed gaping security holes that could be exploited by those looking to disrupt voting by locking up and ransoming voter rolls or simply cutting power at critical polling centers on Election Day. And while large-scale hacking of voting machines is difficult, it is by no means impossible.

There are also weak points up and down the long chain of websites and databases used to tally and report votes, officials said. Run by states or counties, the systems that stitch together reports from thousands of polling centers are a hodgepodge of new and old technologies, many with spotty security.

With the first primaries just weeks away, officials are keeping a watchful eye for hints about what to expect come November. The widespread expectation is that hackers, who may have only a single shot at exploiting a particular bug or vulnerability, will wait until the general election rather than risk wasting it on a primary.

Some of the meddling is homegrown. Americans have been exposed spinning up fake websites for Democratic front-runners and paying Macedonians to promote divisive political views. Facebook, the most important digital platform for political ads, also made it clear this week that it would not police political messaging for lies or misleading claims.

With Americans so mistrustful of one another, and of the political process, the fear of hacking could be as dangerous as an actual cyberattack — especially if the election is close, as expected. That is what happened last November in Kentucky, when talk of a rigged election spread online after it became clear that the governor's race would come down to the wire.

"You don't actually have to breach an election system in order to create the public impression that you have," said Laura Rosenberger, director of the Alliance for Securing Democracy, which tracks Russian disinformation efforts.

"Chaos is the point," she added. "You can imagine many different scenarios."

Still, officials say, the deepest challenges come from abroad. Iran, under harsh sanctions that were not in place four years ago, nosed around the election system in 2018. More recently, Iranian hackers have been caught trying to compromise President Trump's campaign and impersonating American political candidates on Twitter.

For his part, Mr. Trump has already warned North Korea against "interference," though he appeared to be referring to missile launches meant to embarrass him.

The president has shown far less concern about Russian interference. He has repeatedly questioned the idea that Moscow meddled in the 2016 election, viewing such talk as a challenge to his legitimacy. In his zeal to find another culprit, Mr. Trump eagerly embraced a Russian-backed conspiracy theory that shifted the blame to Ukraine, and set in motion the events that led to his impeachment.

American officials, however, are nearly unanimous in the conclusion that Russia interfered in 2016, and that it remains the greatest threat in 2020. Unlike other countries, which are seen as eager to influence American policy, Russia appears, above all, to be interested in undermining confidence in America's democratic institutions, starting with the voting process.

Then and now, officials and experts said, the Russians and others could bank on one constant: America's partisan divide, which engenders deep cynicism among Democrats and Republicans alike.

"Our adversaries, including Russia, China, Iran and others, are persistent: They focus on our politics and try to take advantage of existing fissures and American sentiment, particularly if it may weaken us," said Shelby Pierson, who monitors election threats at the Office of the Director of National Intelligence.

"They'll try many tactics and can adapt," she added. "If it doesn't work out, they try something else."

Live Updates From the Campaign Trail in Iowa

13m ago What happened last night?

24m ago A New York Times analysis finds many errors in the Iowa results.

29m ago Bernie Sanders has a huge January haul.

See more updates

Digital Disenfranchisement

In the public imagination, the defining elements of Moscow's interference in the 2016 election were disinformation and the hacking of Democratic Party emails. But as they look to 2020, many election security officials and experts say the most worrying piece of the Russian meddling was the hacking of state election systems.

Election systems in all 50 states were targets of Russian hackers in 2016, though voting went smoothly in most places. In the estimation of many officials and experts, the effort was probably a trial run meant to probe American defenses and identify weaknesses in the vast back-end apparatus — voter-registration operations, state and local election databases, electronic poll books and other equipment — through which American elections are run.

One expert told the Senate Intelligence Committee that Russia was "conducting the reconnaissance to do the network mapping, to do the topology mapping, so that you could actually understand the network, establish a presence so you could come back later and actually execute an operation."

Of particular concern is the Russians' hacking of three companies that provide states with the back-end systems that have increasingly replaced the thick binders of paper used to verify voters' identities and registration status.

Current and former officials say American intelligence agencies determined in 2017 that the companies' systems had been penetrated. But officials still cannot say how far the hackers got or whether any data was stolen or corrupted.

The companies operate without federal oversight — it is states, after all, that run American elections, yet most lack the resources or expertise to oversee what are essentially tech firms. As a result, little is known about the companies' security, employee requirements or supply-chain practices, experts said.

One of the targeted companies, VR Systems, provided e-poll books to Durham County, N.C., where malfunctions with the electronic systems in 2016 led to scores of voters' being told incorrectly that they had already cast ballots or were ineligible to vote.

Though officials declassified a report in recent weeks that showed configuration errors, not an attack, were to blame for the problems in Durham, experts say the Election Day chaos there highlighted the risk of an attack or ordinary malfunction that blocks voters from casting their votes in swing states.

The rise of ransomware — which typically locks a system until victims pay the attackers in a cryptocurrency like Bitcoin — has given another weapon to attackers looking to sow chaos and digitally disenfranchise voters.

American cities and towns faced a record number of ransomware attacks last year, with more than 100 federal, state and municipal governments hit.

Homeland Security officials are investigating whether Russian intelligence was involved in any of the attacks, according to two department officials who spoke on the condition of anonymity to discuss sensitive intelligence. They are looking into whether cybercriminals, who appeared to be motivated by greed, were used as decoys to test the defenses of states and cities that might make ideal targets closer to the election. Among the towns hit hardest by ransomware last year was Riviera Beach, Fla., in Palm Beach County — which played an outsize role in deciding the contested 2000 presidential election.

President Benedict Arnold

In the immediate aftermath of the 2016 election, there was an intense focus on America's voting machines, particularly the pricey touch-screen devices that lack the paper trail necessary to audit random samples of the tallies or conduct a reliable — if slow — manual recount.

Yet many machines remain vulnerable, as J. Alex Halderman, a professor at the University of Michigan, often demonstrates when he runs fake elections between George Washington and Benedict Arnold, and manipulates the software that prepares the ballots to assure a victory for America's most famous traitor.

"In every single case, we found ways for attackers to sabotage machines and to steal votes," he told the Senate Intelligence Committee, describing his research.

A study published in December by Interos, a risk-management firm, raised questions about the security of the hardware used in the machines, as well. Two-thirds of the companies that supply critical components for voting machines maintain offices in Russia and China, where foreign companies are regularly required to give security officials sensitive technical information, including software code in some cases. Chinese-owned companies make about a fifth of the voting machine components.

Each of those parts presents an opportunity for foreign interference. "There has been insufficient attention to the potential problems of the actual voting machines being hacked," said David Dill, founder of the Verified Voting Foundation.

Come November, seven or so states will still be without full paper backup, including some that are out of funds to replace paperless machines.

Baiting Outrage

Much as 20th-century militaries learned to combine soldiers, sea power and airplanes to mount a coordinated assault, Russia has proved adept at meddling in elections by blending different types of digital malfeasance into one larger operation. The 2016 election exemplified the playbook: Russian hackers stole sensitive material, starting with Democratic Party emails, then used trolls to spread and spin the material, and built an echo chamber to widen its effect.

Now, as the next election approaches, hackers appear to be laying the groundwork for a repeat. But this time they are employing techniques that are more sophisticated — and dangerous — in their attempts to steal potentially embarrassing material from political campaigns.

Security experts say they are witnessing a significant ramp-up in attempts to hack Democratic front-runners. In just the last two months, there were roughly a thousand phishing attempts against each of the leading Democratic candidates, according to Area 1, a Silicon Valley security firm, which did not name the candidates.

Most were attempts to replicate the 2016 hack of Hillary Clinton's campaign chairman, John Podesta, who was successfully baited into turning over his email credentials, said Oren Falkowitz, Area 1's chief executive. But in about a fifth of the attacks, hackers compromised the accounts of campaign consultants and affiliates, and used those to send malicious lures to people inside the campaign. It is an extra step for hackers, but individuals are softer targets than the campaign, and people are far more likely to click on a link if they know the sender.

An episode during the run-up to Britain's recent parliamentary election highlighted the potential, but also the limits, of disinformation campaigns based on real information.

In November, an anonymous Reddit user — who has since been linked to a wide-ranging Russian disinformation campaign — posted internal British government documents that detailed preliminary talks with the United States on a trade deal. Though the post did not gain much attention initially, it eventually made its way to the opposition Labour party, which said it offered proof that the Conservatives, if re-elected, planned to privatize the National Health Service as part of a deal with the United States.

News of the documents forced Prime Minister Boris Johnson to deny that his party planned to privatize the health service, though his government acknowledged that the leaked materials were genuine.

But with the Conservatives well ahead in the polls, the episode did nothing to alter the election's outcome. Mr. Johnson won a commanding majority in Parliament and a clear mandate to proceed with Britain's exit from the European Union — and cut a trade deal with the United States.

The other pieces of the Russian campaign, which targeted a number of Western countries between 2016 and 2019, had even less impact, according to a report last month by Graphika, a firm that tracks social media activity. Called Secondary Infektion, the campaign was run by trolls who used hundreds of social media accounts to spread 44 stories in at least six languages. The stories ranged from fictitious claims about the 2016 American election to an article that sought to link President Emmanuel Macron of France to Islamist militants.

Most were demonstrably false and based on faked interviews or manufactured documents. The trade-deal story appears to have been the only one based on real material, and the only one that made international headlines.

"Some were openly mocked by real users; many were simply ignored," Ben Nimmo of Graphika wrote in the firm's report.

"As the 2020 U.S. presidential election approaches," Mr. Nimmo added, "it is vital to be wary of potential interference, but it is equally important to understand what forms of interference are most damaging."

Pete Buttigieg

Tulsi Gabbard

Amy Klobuchar

Bernie Sanders

Tom Steyer

Elizabeth Warren

Andrew Yang

Keep Up With Our Coverage

- Get an email recapping the day's news
- Download our mobile app on iOS and Android and turn on Breaking News and Politics alerts