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

POLITICS

The Fake Americans Russia Created to Influence the Election

By SCOTT SHANE SEPT. 7, 2017

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.

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.

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.

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.

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:

@edanur01 #WarAgainstDemocrats 17:54

@efekinoks #WarAgainstDemocrats 17:54

@elyashayk #WarAgainstDemocrats 17:54

@emrecanbalc #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 #ClintonCurruption, and used to promote the Russian 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 said 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."

A version of this article appears in print on September 8, 2017, on Page A1 of the New York edition with the headline: To Sway Vote, Russia Used Army of Fake Americans.