ALTERNET
The Conversation
July 28, 2018

An Ethical Hacker Explains How the Russian Government Used Disinformation and Cyber Warfare in the 2016 Election

Cybersecurity experts in the US knew about Russian intelligence agencies' activities, but may not have had any idea how comprehensive and integrated they were – until now.

Photo Credit: Image by Shutterstock, Copyright (c) Glebstock

The Soviet Union and now Russia under Vladimir Putin have waged a political power struggle against the West for nearly a century. Spreading false and distorted information – called "dezinformatsiya" after the Russian word for "disinformation" – is an age-old strategy for coordinated and sustained influence campaigns that have interrupted the possibility of level-headed political discourse. Emerging reports that Russian hackers targeted a Democratic senator's 2018 reelection campaign suggest that what happened in the lead-up to the 2016 presidential election may be set to recur.

As an ethical hacker, security researcher and data analyst, I have seen firsthand how disinformation is becoming the new focus of cyberattacks. In a recent talk, I suggested that cyberwarfare is no longer just about the technical details of computer ports and protocols. Rather, disinformation and social media are rapidly becoming the best hacking tools. With social media, anyone – even Russian intelligence officers and professional trolls – can widely publish misleading content. As legendary hacker Kevin Mitnick put it,

> "it's easier to manipulate people rather than technology."

Two sets of federal indictments – one in February and another in July – allege in detail how a private company linked to Putin and the Russian military itself worked to polarize American political discourse and sway the 2016 U.S. presidential election.

Cybersecurity experts in the U.S. knew that the Russian intelligence agencies were conducting these acts of information warfare and cyberwarfare, but I doubt they had any idea how comprehensive and integrated they were – until now.

Russia's propaganda machine duped American voters

The operation was complex. What is publicly known now is perhaps most easily understood in two pieces, the subjects of separate federal indictments.

First, a billionaire Russian businessman and Putin associate allegedly assembled a network of troll factories: private Russian companies engaging in a massive disinformation campaign. Their employees posed as Americans, created racially and politically divisive social media groups and

pages, and developed fake news articles and commentary to build political animosity within the American public.

Second, the Russian military intelligence agency, known by its Russian acronym as the GRU, allegedly used coordinated hacking to target more than 500 people and institutions in the United States. The Russian hackers downloaded potentially damaging information and released it to the public via WikiLeaks and under various aliases including "DCLeaks" and "Guccifer 2.0."

Online trolls manipulated your opinions

The people involved did not fit the stereotypical picture of internet trolls. One leading Russian troll factory was a company called the Internet Research Agency, reportedly with all the trappings of a real corporation, including a graphics department to create incendiary images, a foreign department dedicated to following political discourse in other countries and an IT department to make sure trolls had reliable computers and internet connections. Employees, mostly 18 to 20 years old, were paid as much as US$2,100 a month for creating fake social media accounts and blogs to distribute disinformation to Americans.

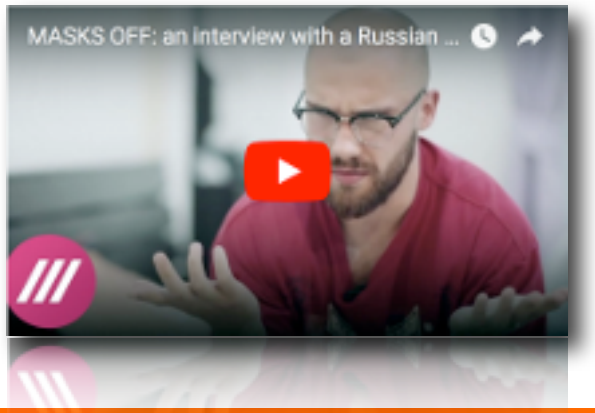
They were employed to take advantage of deepening political polarization in the U.S. The Russians saw this as an opportunity to stir up conflict – like poking a stick into a beehive. These trolls were instructed to stir up racial tensions, stage "flash mobs" and organize activist campaigns – sometimes announcing events for opposing groups at the same times and locations.

One ex-troll told a Russian independent TV network that his job included writing incendiary comments and creating fake posts on political forums:

> "The way you chose to stir up the situation, whether it was commenting [on] the news section or on political forums, it didn't really matter."

In 2015, well before the 2016 election, the troll-factory network had more than 800 people doing this kind of work, producing propaganda videos, infographics, memes, reports, news, interviews and various analytical materials to persuade the public.

America never stood a chance.



Essayez de regarder cette vidéo sur www.youtube.com

https://youtu.be/wAUIOrHD-sM

An interview with an ex-Russian troll.

Focusing on social media

It's no surprise that these Russian trolls spent most of their time on Facebook and Instagram: Two-thirds of Americans get at least some news on social media. The trolls spread out across both platforms, seeking to encourage conflict on any topic that was getting a lot of attention: immigration, religion, the Black Lives Matter movement and other hot-button issues.

When describing how he managed all of the fake social media accounts, the ex-troll said:

> "First, you gotta be a redneck from Kentucky, then you need to be a white guy from Minnesota, you've slaved away all your life and paid your taxes, and then 15 minutes later you are from New York posting in some Black slang."

Then, the indictments reveal, the GRU entered this increasingly fraught online political discourse.

The GRU joins in

Like another significant political scandal, the GRU effort allegedly started with a break-in to Democratic National Committee records – but this time it was a digital burglary. It wasn't particularly sophisticated, either, using two common hacking techniques, spearphishing and malicious software.

As the July indictment details, starting in March 2016, Russian military operatives sent a series of fake emails, disguised to look real, to more than 300 people associated with Democratic National Committee, the Democratic Congressional Campaign Committee and Hillary Clinton's presidential campaign. One of the targets was Clinton campaign chairman John Podesta, who fell for the scheme and unwittingly handed over more than 50,000 emails to the Russians.

Around the same time, the Russian hackers allegedly began searching for technical vulnerabilities in the Democratic organizations' computer networks. They used techniques and specialized malicious software that Russians had used in other hacking efforts, including against the German Parliament and the French television network TV5 Monde. By April 2016, the hackers had gained access to the Democratic Congressional Campaign Committee systems, exploring servers and secretly extracting sensitive data. They located a Democratic Congressional Campaign Committee staffer who also had privileges in the Democratic National Committee systems, and thereby got into the Democratic National Committee networks too, extracting more information.

When the Democratic National Committee realized there was unusual data traffic in its systems, the group hired a private cybersecurity firm, which in June 2016 publicly announced that its investigation had concluded that Russia was behind the hacking. At that point, the Russians allegedly tried to delete traces of their presence on the networks. But they kept all the data they had stolen.

Opposing Hillary Clinton

As early as April 2016, the GRU was allegedly trying to use the Democrats' confidential documents and email messages to stir up political trouble in the U.S. There is evidence that the Russian government, or people acting on its behalf, offered key people in the Trump campaign damaging information on Clinton.

In July 2016, the indictments say, the GRU began releasing many of the Democrats' documents and email messages, mainly through WikiLeaks, an internet site dedicated to anonymous publishing of secret information.

All of this effort was, according to the indictments, set up to undermine Hillary Clinton in the eyes of the American public. Putin definitely wanted Trump to win – as the Russian president himself acknowledged while standing next to Trump in Helsinki in July. And the trolls were instructed to go after her savagely: A former Russian troll said,

> "Everything about Hillary Clinton had to be negative and you really had to tear into her. It was all about the leaked email, the corruption scandals, and the fact that she is super rich."

The indictments describe in detail how information warfare and cyberwarfare were used as political tools to advance the interests of people in Russia. Something similar may be set to happen in 2018, too.

❒ Timothy Summers, Director of Innovation, Entrepreneurship, and Engagement, College of Information Studies, University of Maryland

❒ This article was originally published on The Conversation.

❒ Read the original article.