Testimony of Philip N. Howard, Oxford University

“Foreign Influence on Social Media Platforms: Perspectives from Third-Party Social Media Experts”

Senate Select Committee on Intelligence, Open Hearing, August 1, 2018

Thank you, Chairman Burr and Vice Chairman Warner, for the opportunity to testify on foreign influence operations and their use of social media platforms.

My name is Phil Howard; I am a Professor at Oxford University and Director of the Oxford Internet Institute, an academic department of Oxford University. My areas of expertise include political communication and international affairs.

There is a significant amount of punditry and speculation about the role and impact of foreign influence operations and their use of social media platforms. I tend to work with open-source information, public archives, and the feeds of data that the social media platforms make available. I think I can best serve you by sticking close to evidence that has either come (1) from my own research team at Oxford University or (2) from the network of academics who are evaluating foreign influence on social media platforms.

OUR RESEARCH FINDINGS

At the Oxford Internet Institute, I have been leading the Project on Computational Propaganda, which is currently funded by the European Research Council. I began working on this in 2010 with the support of the National Science Foundation, and our research team was the first large-scale, dedicated effort to study the role of disinformation and social media manipulation in public life.

We coined the term “computational propaganda” because this kind of disinformation is unique: it makes use of automation, algorithms and big-data analytics to manipulate public opinion in targeted ways. The term encompasses political content falsely packaged as news, the spread of misinformation on social media platforms, illegal data harvesting and micro-profiling, the exploitation of social media platforms for foreign influence operations, the amplification of hate speech or harmful content through fake accounts or political bots, hacking and social engineering, and clickbait content for optimized social media consumption. Computational propaganda is often illegal under the existing rules of elections administration that most democracies have in place.

Based on publicly available data, including the small amounts of data that the social media firms released last summer, there are several things we know about the strategies that Russian operators employ and which US voters they seek to influence. Our team has worked with data on the accounts that the social media platforms have exposed as managed by Russian operators. We know what messages these accounts sent and what advertisements these users bought and then targeted at US voters.

From this evidence, we can identify several kinds of computational propaganda campaigns.

1. **Campaigns to polarize voters on particular issues.** For example, known Russian social media accounts will simultaneously promote political action by a group called “United Muslims of America” and the “Army of Jesus”, or encourage African American political actives around “Black Lives Matter” and then develop a “Blue Lives Matter” movement. The goal is to get groups of voters to confront each other angrily, over social media and in the streets. Video content, edited and taken out of context, makes new immigrants seem like a threat to veterans, or tells one community that the police need our support while telling another that police are abusing them.

2. **Campaigns to promote or discredit particular Senators, Presidential candidates, and other public figures.** Foreign-backed rumor-mongering is not new, but it is much more strategically targeted within districts and by voter demographics than before. It is safe to say that every public figure on the national stage is either attacked by or benefits from highly automated or fake social media accounts, and whether these campaigns are managed by foreign governments depends on the issues involved and time of the campaign season.

3. **Campaigns to discourage citizens from voting.** Voter suppression is a common messaging strategy, aimed at the voters who might support a candidate that a foreign government finds unpalatable. For example, voters are often told that voting day has been postponed, or that they can text message their vote in, or that their polling station has moved.

It is difficult to know how many people in the United States have seen such messages, or how many voters were actually influenced by them. Only the social media firms themselves could share that data or estimate those probabilities accurately. But, in the US context, it is safe to assume that social media platforms efficiently delivered these messages and advertisements to voters, and that these messages had an influence, in different ways, in different states, and in conjunction with all the other variables that shape an electoral outcome.

**THE UNITED STATES AS A TARGET**

We have demonstrated that, during the last Presidential election, there was a one-to-one ratio of junk news to professional news shared by voters over Twitter. In other words, for every one link to a story produced by a professional news organization there was one link to content that was extremist, sensationalist, conspiratorial or other form of junk news. Not only is this the highest level of junk news circulation in any of the countries we have studied, but this misinformation was actually concentrated in swing states. Disinformation campaigns are often launched with highly automated accounts and fake users, and these kinds of accounts pushed significant amounts of content from Russian news sources, links to unverified content on WikiLeaks, and other junk news. Our analysis demonstrates that this

---

content does not simply flow across networks of bots—at the right volume level it can permeate deeply into networks of human users.⁴

These operations are ongoing. Months after the last major election in the US, we demonstrated that disinformation about national security issues, including from Russian sources, was being targeted at US military personnel, veterans, and their families.⁵ During the President’s State of the Union address, we learned that junk news is particularly appetizing for the far right, white supremacists, and President Trump’s supporters (though not “small c” conservatives).⁶ Some of this junk content actually originates with accounts managed by foreign governments.

**INFLUENCE OPERATIONS GLOBALLY**

Our team recently completed a second global inventory of the organizational capacity of different governments and political parties to manipulate public opinion over social media. Around the world, a range of government agencies and political parties are exploiting social media platforms to spread junk news and disinformation, exercise censorship and control, and undermine trust in the media, public institutions, and science. At a time when news consumption is increasingly digital, artificial intelligence, big-data analytics, and “black-box” algorithms are being leveraged to challenge truth and trust. These are cornerstones of democracy.

In 2017, [our first global cyber troops inventory](#) shed light on the global organization of social media manipulation by government and political party actors.⁷ Now, only a year later, we find a significant expansion of this capacity.⁸

1. We have found evidence of formally organized social media manipulation campaigns in 48 countries, up from 28 countries last year. In each country, there is at least one political party or government agency using social media to manipulate public opinion domestically.
2. Much of this growth comes from countries where political parties are spreading disinformation during elections, or countries where government agencies feel threatened by junk news and foreign interference and are responding by developing their own computational propaganda campaigns in response.

---

3. In a fifth of these 48 countries—mostly across the Global South—we found evidence of disinformation campaigns operating over chat applications such as WhatsApp, Telegram and WeChat.

4. Computational propaganda still involves social media account automation and online commentary teams, but is making increasing use of paid advertisements and search engine optimization on a widening array of Internet platforms.

5. Social media manipulation is big business. Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media. In a few countries this includes efforts to counter extremism, but in most countries this involves the spread of junk news and misinformation during elections, military crises, and complex humanitarian disasters.

RESEARCH ON VOTER IMPACT

Some of the best evidence about social media advertising and influence comes from the platforms themselves. A growing number of researchers work with social media data over polling data to answer basic research questions about public opinion dynamics.\(^9\) Social media are not only important for obtaining news and political content, but also as an indicator of public sentiment in elections and other political crises.\(^10\) No matter the platform, social media users are producing a vast amount of data that is collected and analyzed to generate detailed psychological profiles of users that can provide insight into attitudes, preferences, and behaviors. Indeed, the successful business model of these firms is to algorithmically connect users to content that is relevant to them individually, as well as target them with personalized advertising, using systems that political actors can “pay to play” in. The information users produce about themselves online helps craft the computational propaganda they are subsequently sent, influencing voting behavior and improving voter turnout.\(^11\) The study of news consumption habits of social media users can also produce fine-grained analyses of the causes and consequences of political polarization.\(^12\)

Social media almost certainly facilitates selective exposure, but more likely through social endorsements rather than simply partisan frames. On Facebook, friends share news from consistent ideological perspectives, rarely using diverse sources of political news and information. In a study by Bakshy et al., Facebook users encountered roughly 15% less cross-cutting content in their news feeds due to algorithmic ranking, and clicked through to 70% less of this cross-cutting content.\(^13\) Within the domain of political news encountered in social media, selective exposure appears to drive attention. However, the underlying driver of attention is the social endorsement that is communicated through the act of sharing: social media users will not pay attention simply because a piece of political news is from a

---


13 Bakshy, Messing, and Adamic.
credible source or generated by a political party, they pay attention because someone in their social network has signaled the importance of the content.\textsuperscript{14} Other researchers have found that when the top search results about a political leader are positive, people say they will vote for that person. When they are shown negative results, people report that they less likely to vote.\textsuperscript{15} So it should not be surprising that foreign governments seeking to interfere with domestic politics and shape public opinion inside a country would put resources into manipulating search results.

CONCLUSION: WHAT IS NEXT?
Disinformation campaigns will continue to be launched against voters in democracies. For every new social media platform, every new design idea on every platform, and every new digital device, someone will work to integrate the innovation with a computational propaganda campaign.\textsuperscript{16}

First, globally, we can expect a growing number of foreign powers to develop disinformation campaigns for single issues and legislative campaigns, not just elections.

Second, globally, we can expect foreign governments to apply these techniques and develop these messages for multiple platforms. They will to whatever social media platform has voters.

Third, globally, we can expect advances in artificial intelligence and machine learning to be used to support ever more individuated campaigns. Currently, foreign influence operations take advantage of the algorithms built by social media firms and search engines to customize the delivery of disinformation. Artificial intelligence, machine learning, and natural language processing will not only be used for individual targeting, but individually customized content. Videos and text can be crafted by knowledge of credit card purchases, and device data from our mobile phone, or from our “Internet of Things” refrigerator.

Fourth, globally, we can expect regimes other than Russia to develop their capacity to influence domestic public opinion. We believe China has significant capacity, but have only caught their influence operations against Taiwan and the Chinese diaspora. Authoritarian governments tend to learn from each other, and we have seen more and more such regimes applying these techniques.

Fifth, within the United States, we can expect the same kinds of voters to continue to be targets for misinformation. Given the disinformation campaigns which have been—and are currently—running, I would guess that foreign actors will continue to aim future disinformation campaigns at African American voters, Muslim American voters, White Supremacist voters, and voters in Texas and the Southern States. I expect the strategy will remain the same: push disinformation about public issues; discredit politicians and experts; and prevent particular types of voters from participating on Election Day.

\textsuperscript{16} Philip N. Howard, \textit{Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up} (New Haven, CT: Yale, 2015).
The manipulation of public opinion over social media platforms has emerged as a critical threat to public life. The solution to these problems necessarily involves research and public policy oversight. Technology firms occasionally share small amounts of data, but providing a regular flow of data about public life to elections administrators, researchers, and civil society groups is the best way to ensure that social media firms make good decisions and design their platforms to support and defend, rather than undermine and expose, our democratic institutions.
REFERENCES


