OCTOBER 2020

Election 2020: Foreign Interference and Domestic Manipulations Aimed at Voters and Electoral Outcomes

By Marietje Schaake and Rob Reich

IN 2016 WE LEARNED ABOUT EFFORTS BY FOREIGN ACTORS to interfere in the U.S. election by injecting misinformation and disinformation into public discourse on social media. False events and personas added to the polarization and manipulation of voters.

The 2020 election is marked by similar efforts, though this time the actors are domestic as well as foreign. What do we do know about people with deceptive or malicious agendas trying to influence citizens ahead of elections, to degrade democracy and sow distrust in the election results, or to spread confusion about science and facts more generally through our information systems?

KEY TAKEAWAYS

- Due to free speech safeguards, it is more difficult to regulate domestic actors manipulating information online.
- Content moderation enforcement is quite uneven across social media platforms, with the larger firms often able to spend much more than smaller ones.
- Bipartisan policy opportunities to address election security issues may be more likely in 2021, a non-election year at the U.S. national level.

Stanford University
Human-Centered
Artificial Intelligence

Stanford | Cyber Policy Center
Freeman Spogli Institute

Often, it's not a question of "hacking" voting machines, but rather of hacking the minds of voters to induce them to take voting actions – or to refrain from voting altogether. The 2016 election stands as a prime example – multiple Russian efforts were aimed at interfering in that year's presidential election and hurting Democrats. This included creating division across social media, hacking and leaking emails, and tempting media outlets into spreading such narratives.

Foreign and domestic electoral manipulation is one of the topics in the eight-week Stanford University course, "Technology and the 2020 Election: How Silicon Valley Technologies Affect Elections and Shape Democracy." This joint class for Stanford students and Stanford's Continuing Studies Community enrolls a cross-generational population of more than 400 students from around the world.

The class session on "Manipulation: Misinformation and Disinformation" included guest experts Camille Francois, research affiliate at Harvard University's Berkman Klein Center for Internet and Society and chief innovation officer at Graphika, and Alex Stamos, director of the Stanford Internet Observatory and former chief security officer at Facebook. Both are involved in the Election Integrity Partnership, a coalition of research entities focused on supporting real-time information exchange between the research community, election officials, government agencies, civil society organizations, and social media platforms. Lisa Einstein, course manager to Rob Reich and Marietje Schaake and a Stanford master's degree candidate in computer science, also contributed to this issue brief and discussion below.

Introduction

When Alex Stamos was working at Facebook, he discovered that about $100,000 in ad spending was affiliated with Russian sources from June 2015 to May of 2017 and connected to hundreds of inauthentic accounts and pages. Some of these efforts were aimed at the Black Lives Matter movement, rather than focusing on support for particular candidates. Overall, these Russian-manipulated ads attempted to amplify divisive social and political messages across the political spectrum on issues such as LGBTQ rights, race, immigration, and gun rights. The ads were designed to foment more polarization along existing political fault lines in the United States and to further radicalize certain groups.

When then-presidential candidate Donald Trump claimed in a debate that the Democratic National Committee hack involving John Podesta's emails could have been executed by someone in their bed weighing 400 pounds, he played directly into Russian President Vladimir Putin's playbook by forcing Americans to question the credibility of their own democratic process.

The pandemic has opened a new front in the misinformation and disinformation battle. The discrediting of established voices on science, such as the World Health Organization or the Centers for Disease Control and Prevention, produces an information environment in which growing numbers of people question authoritative sources of science and fact.

The result is a proliferation of misinformation and disinformation about COVID-19 that some call an "info-demic." It has effects on peoples' offline behavior and has led to higher infection rates as some have also stopped using or reduced their protective measures against COVID-19.

"Misinformation" includes false content, such as conspiracies, created or disseminated without the intention to mislead or harm people. "Disinformation" is false information created or disseminated with the conscious intention to mislead or harm. A related phenomenon is the creation of "deep fakes," which are manipulated images or video. Such "synthetic media" creates new opportunities of disinformation that will further undermine trust, even in our own senses. What we see with our own eyes may not be believable.

For foreign interference, we are on much better footing than in 2016. This doesn't mean there is no threat, but collectively, we are much better prepared.

Discussion

Though the twin events of a crucial election and global pandemic have led some social media platforms to take more proactive stances than ever before to moderate health and election-related disinformation, the problem of disinformation continues to grow in sophistication.

In the U.S., some elected officials – including the President himself – are spreading rumors or falsehoods to deter people from voting and to pre-emptively delegitimize election results. While democratic regulation is legitimate, some political leaders are creating "fake news" laws and policies as excuses to silence opponents and political rivals – or to impose internet shutdowns during contentious political events.

Though the U.S. might be more prepared for disinformation campaigns during the 2020 election than in 2016, this has not yet deterred manipulative efforts. For example, U.S. intelligence recently pointed to foreign state actors such as Iran as the likely sources of emails claiming to be linked to the "Proud Boys" and sent to American voters threatening to hurt them if they wouldn't vote for Donald Trump. Even though the emails were sent to an estimated couple thousand voters, the effort garnered significant American media attention.

This in turn raises another concern: when disinformation creates a media buzz and repetition of

the very falsehoods involved. Editorial boards, such as that of the Washington Post, have now published editorial guidelines on how they will report about disinformation. This is an advisable process, lest the press become a main vector for the dissemination of disinformation.

It's important to understand which audiences disinformation campaigns are targeting. Some are extremely elaborate, taking place over a half dozen years, wherein a foreign actor creates multiple personae and builds influence in online groups. Offline effects, such as how these efforts then lead to events and organizing, need to be better understood. Access to relevant data from platform companies is urgently needed for such independent research.

Social scientists, meanwhile, have much fertile ground to explore regarding the concrete effects of disinformation – the 2020 election might well yield a lot of data on this subject. In developing countries, disinformation is an ongoing problem that goes little noticed in the U.S., even though important lessons could be ascertained from experiences in the rest of the world. It is a reminder that standards set by Silicon Valley giants impact people all over the globe.

In the U.S., the federal government has a variety of tools at its disposal to thwart foreign interventions, which do not enjoy First Amendment protections and are subject to electoral campaign laws. In the case of domestic actors, it's more difficult to regulate their online activity due to free speech safeguards. And, Section 230 of the Communications Decency Act generally provides immunity for social media platforms from third-party content.

For election security, we expect the equivalent of a local sheriff's office to go up against a foreign military. This is a problem. We've distributed responsibility down to people who are not able to stand up against professional adversaries. This has to get fixed in the next Congress.

However, understanding the various aspect of disinformation campaigns requires not only looking at content, but also at actors and their behavior, as Camille Francois explains in the ABC framework she presented last September to the U.S. House of Representatives.

Content moderation enforcement is quite uneven across social media platforms, with the larger and more

visible firms often doing much more than smaller ones. Available resources to invest are one reason. Finally, the attention on foreign-sourced disinformation has distracted many from the quite considerable number of homegrown or domestic manipulators, who may act out of political or commercial motives. And, the hypothetical scenario of an alleged hack into the vote count in several swing states on election day indicates the real-world implications for handling such disinformation on a timely basis.

Disinformation won't go away. This is the price of living in an open society. With a free press and an unregulated internet, we're going to live with the possibility of foreign and domestic actors injecting disinformation into our environment.

Final Thoughts

In regard to the 2020 election and the role of non-governmental civil organizations, which enjoy some flexibility compared to state entities, The Election Integrity Partnership's objective is to detect and reduce the impact of attempts to prevent or deter people from voting or to delegitimize election results. They can provide rapid responses in such instances to social media platforms and election offices.

Bipartisan policy opportunities to address these election security issues may be more likely in 2021, a non-election year at the U.S. national level. A policy framework should take into account the global nature of the problem. Democratic societies may have to live with disinformation to a certain extent as the cost of living in free and open communities. But that does not mean the business models that facilitate manipulation should be left unregulated. To combat disinformation, governments, policymakers and social media platforms need to pay more attention to the problems that arise in order to avoid worst scenarios. And, while political candidates often rhetorically disavow such manipulations, they need to directly call upon their supporters to disengage from these efforts.

ELECTION 2020: FOREIGN INTERFERENCE AND DOMESTIC MANIPULATIONS AIMED AT VOTERS AND ELECTORAL OUTCOMES

Stanford University's Institute for Human-Centered Artificial Intelligence (HAI), applies rigorous analysis and research to pressing policy questions on artificial intelligence, particularly human-centered AI technologies and applications.
For further information, please contact HAI-Policy@stanford.edu.

The Cyber Policy Center at the Freeman Spogli Institute for International Studies is Stanford University'' premier center for the interdisciplinary study of issues at the nexus of technology, governance and public policy.

The views expressed in this issue brief reflect the views of the authors.

Rob Reich is a professor of political science at Stanford University. He is also the associate director of Stanford's Institute on Human-Centered Artificial Intelligence, director of the Center for Ethics in Society, and faculty co-director of Stanford's Center on Philanthropy and Civil Society. His new book, *Digital Technology and Democratic Theory*, will be published in December.

Marietje Schaake is the international policy director at Stanford's Cyber Policy Center and international policy fellow at Stanford's Institute for Human-Centered Artificial Intelligence. President of the Cyber Peace Institute, Marietje served between 2009 and 2019 in the European Parliament, focusing on trade, foreign affairs and technology policies.

Stanford University
Human-Centered
Artificial Intelligence

Stanford HAI: Cordura Hall,
210 Panama Street, Stanford, CA 94305-1234
T 650.725.4537 **F** 650.123.4567
E HAI-Policy@stanford.edu **hai.stanford.edu**

Stanford | Cyber Policy Center
Freeman Spogli Institute

Stanford Cyber Policy Center: Encina Hall
616 Jane Stanford Way, Stanford, CA 94305-6055
T 650.724.6814 **E** cyber-center@stanford.edu
stanfordcyber.org