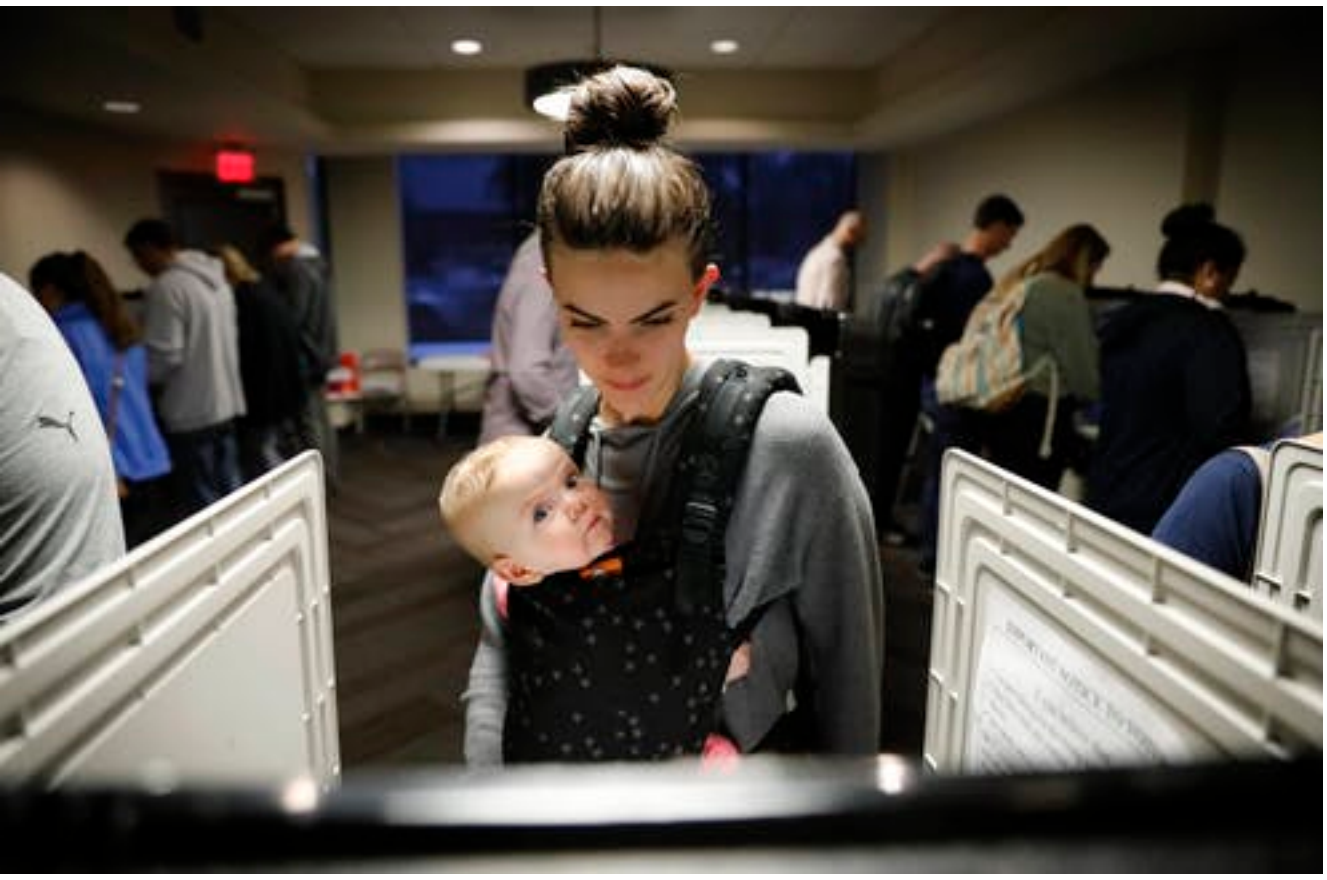
THE CONVERSATION

Academic rigor, journalistic flair



As Americans go to the polls, the voting process and the information environment are still not secure. AP Photo/David Goldman

Threats remain to US voting system – and voters' perceptions of reality

November 6, 2018 2.52pm EST

Author

Richard Forno

Senior Lecturer, Cybersecurity & Internet Researcher, University of Maryland, Baltimore County

As the 2018 midterms proceed, there are still significant risks to the integrity of the voting system – and information warfare continues to try to influence the American public's choices when they cast their ballots.

On the day of the election, there were a number of early hitches in voting at individual polling places, such as polling places opening late and vote-counting machines not plugged in. But there seem not – at least not yet – to be major problems across the country.

However, not all the election-related news and information voters have been encountering in recent days and weeks is accurate, and some of it is deliberately misleading. As this election's results come back, they will reveal whether the misinformation and propaganda campaigns conducted alongside the political ones were effective.

Securing election systems

America's electoral process remains highly fragmented, because of the country's cherished tradition of decentralized government and local control. While this may leave some individual communities' voting equipment potentially vulnerable to attack, the nation's voting process overall may be more trustworthy as a result of this fragmentation. With no unified government agency or office to provide, administer and protect election technologies, there's not one central national element that could fail or be attacked.

Across the country, though, many districts' voters will cast ballots with the help of machines that have long-standing security concerns. Fortunately, 45 states keep a paper record of each vote cast – whether for fear of threats to voting integrity or just budget constraints preventing purchase of newer gear. But that means five states – Louisiana, Georgia, South Carolina, New Jersey and Delaware – don't keep paper records of their voters' choices.

Voting machine vendors have been reluctant to appear before Congress to explain their systems' security practices – and shortcomings. However, federal agencies have helped some states reduce the likelihood of voting machines being hacked or physically tampered with.

Beyond voting machines

Election security is about much more than voting machines and vote-counting systems, though they are the most visible technologies at work on Election Day. State systems that track voter registrations, or allow users to register online, are enticing targets for hackers, too. Security firm Carbon Black reported that 81 million voter records from 20 states are available in online forums. This data, obtained by hacking various official and corporate databases, could be used to facilitate voter fraud or sow confusion at polling places on Election Day: How would you feel if you were told that someone using your name and address had already voted?

There are security concerns even in states like Oregon, where everyone votes on paper and mails in their ballots in advance of Election Day. That state's election officials were targeted by hackers seeking to gain access to state email and database systems. With that access, attackers might be able to digitally impersonate a government official to send false or confusing emails, press releases or other notifications to citizens, journalists or poll workers.

Also at risk are public-facing official websites that carry election information. Merely changing the reported location of polling places or voting hours could prevent some people from voting. Also vulnerable are states' methods of announcing preliminary election results. At a major internet security conference in August, children were able to compromise replicas of several states' election-reporting systems. The most remarkable was that in just 10 minutes, an 11-year-old boy cracked the security on a copy of the Florida secretary of state's website and was able to change the publicly announced vote totals for candidates. That could be enough to cast doubt on whatever was later reported as the official results – and the integrity of the system itself.

Managing information on social media

A more difficult threat to defend against is information warfare, which doesn't attack voting machines or election officials' computers. Rather, it targets voters' perceptions and decisions, seeking to influence how they vote.

Long before the 2016 U.S. presidential election, information warfare was influencing elections around the world, including in Ukraine, Myanmar and Egypt. But after 2016, Facebook and Twitter came under intense scrutiny for their role in providing digital environments that facilitated the spread of misinformation to sow discontent, and special counsel Robert Mueller began investigating Russians' influence efforts.

In the run-up to the 2018 midterms, Russians and others were still hard at work trying to influence Americans to vote in ways that help foreign interests. In October, the U.S. Department of Justice charged a Russian woman with creating thousands of fake social media accounts allegedly representing American citizens to "create and amplify divisive social media and political content" before the election.

This year, though, unlike two years ago, social media companies are taking action. Twitter and Facebook have both deleted thousands of accounts they identified as engaging in propaganda and influence-peddling. And they have made other efforts to identify and fight falsehoods on their platforms, too.

Nevertheless, online misinformation continues to thrive. More than 80 percent of the Twitter accounts that often shared links to false and misleading information in 2016 are still active today. And the amount of online misinformation is higher than it was two years ago.

Investigating alleged wrongdoing

U.S. intelligence and police agencies are concerned about the potential effects of misinformation on the American electorate. But large proportions of the country don't trust those organizations to be politically independent. It doesn't help that the White House continues to claim, without evidence, that voter fraud is a significant problem.

Mainstream news organizations can find themselves under scrutiny too, either for reporting falsehoods that appear to gain traction online or for failing to filter out or properly identify inaccurate information for their readers.

Looking ahead

Protecting democracy is a huge challenge. I've written before that it involves more than technical solutions to computer problems. The U.S. government, and the people it serves, must find the desire and the drive to establish secure and trustworthy procedures for running elections across the country. Education is also key, teaching people from an early age how to recognize propaganda and

misinformation, and think critically about the information they encounter. Facts are not subject to alternative views; without widespread agreement on common objective realities, society and government cannot function well.

Technology continues to evolve, presenting challenges to individuals and society alike. Emerging "deepfake" technology is already helping create convincing videos of people appearing to say and do things they never said or did. In addition, intelligent social media bots are becoming more human-like, making identifying and blocking them much more difficult. That's just some of the challenges that democracies will face in the future.

Many of these problems will not have a clearly defined fix, because they involve a nuanced balancing of individual rights and social necessities. Real and lasting solutions must come from civil discourse by rational and objectively informed people who have, above all, the actual honest desire to do it right.

Cybersecurity | Voter registration | Information warfare | Voting security | Misinformation | Election integrity | Social media and democracy | Election security | 2018 midterm elections | Deepfakes | voting integrity