The battle against disinformation is global
20 March 2020, by Scott Shackelford

Disinformation-spewing online bots and trolls from halfway around the world are continuing to shape local and national debates by spreading lies online on a massive scale. In 2019, Russia used Facebook to intervene in the internal politics of eight African nations.

Russia has a long history of using disinformation campaigns to undermine opponents—even hoodwinking CBS News anchor Dan Rather back in 1987 into saying that U.S. biological warfare experiments sparked the AIDS epidemic.

One group of researchers identified Russian interference in 27 elections around the world, from 1991 to 2017. It interfered in the 2016 U.S. elections, reaching more than 126 million Americans on Facebook alone. Russia is almost certainly already doing so again in 2020.

But Russia is not alone: From the end of World War II to the year 2000, scholars have documented 116 attempts to influence elections – 80 of them by the United States.

Nations around the world, including the United States, have to decide how to react. There is no shortage of experimentation, with new laws and codes of conduct, and even efforts to cut off internet access entirely—and that was before misinformation regarding the COVID-19 pandemic.

As a scholar of cybersecurity policy, I have been reviewing the efforts of nations around the world to protect their citizens from foreign interference, while protecting free speech, an example of which is being published by the Washington and Lee Law Review.

There is no perfect approach, given the different cultural and legal traditions in play. But there’s plenty to learn and use to diminish outsiders’ ability to hack U.S. democracy.

Europe

The European Union has been a target of Russian efforts to undermine stability and trust in democratic institutions including elections across Europe.

Disinformation was rampant across Europe in 2019, including in the Netherlands and the U.K., prompting the closing of far-right Facebook groups for spreading “fake news and polarizing content.”

This has been repeated elsewhere in Europe, such as Spain, where Facebook—again under pressure from the authorities and civil society groups—closed down far-right groups’ Facebook pages days ahead of their parliamentary elections in April 2019.

The disinformation efforts go beyond Facebook and manipulated Twitter feeds, when Twitter handles are renamed by hackers to mislead followers. A growing aspect of multiple disinformation is how artificial intelligence can create manipulated videos that look real, which are called deepfakes.

Not all of this interference is foreign, though—political parties across Europe and around the world are learning disinformation tactics and are deploying it in their own countries to meet their own goals. Both the Labour and Conservative parties in
the U.K. engaged in these tactics in late 2019, for example.

In response, the EU is spending more money on combating disinformation across the board by hiring new staff with expertise in data mining and analytics to respond to complaints and proactively detect disinformation. It is working to get member countries to share information more readily, and has built a system that provides nations with real-time alerts of disinformation campaigns. It is unclear if the U.K. will be participating in these activities post-Brexit.

The EU also seems to be losing patience with Silicon Valley. It pressured social media giants like Facebook, Google and Twitter to sign the Code of Practice on Disinformation in 2018. This initiative is the first time that the tech industry has agreed "to self-regulatory standards to fight disinformation." Among other provisions, the code requires signatories to cull fake accounts, and to report monthly on their efforts to increase transparency for political ads.

In response, these firms have set up "searchable political-ad databases" and have begun to take down "disruptive, misleading or false" information from their platforms. But the code is not binding, and naming and shaming violators does not guarantee better behavior in the future.

At the national level, France has taken a leading role in taxing tech giants to reign in the power of tech firms including how they are used to spread disinformation, prompting threats of retaliatory tariffs from the Trump administration. But this may just be a "warmup" to more ambitious actions designed to help protect both competition and democracy.

Asia

Democracies across Asia are also dealing with disinformation.

In Indonesia, for example, President Joko Widodo spearheaded the creation of the new National Cyber and Encryption Agency to combat disinformation in their elections. One example was in June 2019, when a member of the Muslim Cyber Army was arrested in Java for posting misinformation that implied that the Indonesian government was being controlled by China.

Like Indonesia, Malaysia has also criminalized the sharing of misinformation. Myanmar and Thailand have leaned on law enforcement actions by arresting people who they argue are behind disinformation campaigns to curtail misinformation, which have been abused in some cases to silence critics of public corruption.

The problem of disinformation in India is so severe that it has been likened by some commentators to a public health crisis. One Microsoft study, for example, found that 64% of Indians encountered disinformation online in 2019, which was the highest proportion among 22 surveyed countries.

Not only have these incidents affected elections in India such as by spreading false information about candidates on WhatsApp, but they have led to real-world harm, including at least 33 deaths and 69 instances of mob violence following kidnapping allegations.

In response, the Indian government has shut down the internet more than 100 times over the past year, and has proposed laws that would give it largely unchecked surveillance powers, mirroring Chinese-style internet censorship.

Australia and New Zealand

Australia and New Zealand have also been targets of online influence campaigns – not from Russia, but from China. In response, Australia has enacted a new law to ban foreign interference in Australia’s elections, but enforcement has been lacking.

New Zealand has taken on a more global leadership role in combating this problem. In partnership with France, New Zealand’s Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online has more than 50 nations supporting its goal of stopping the spread of violent extremism online and banning foreign political donations. Although not necessarily disinformation, such content can similarly widen fissures in
Making cyberspace safe for democracy

Groups within the U.S. and outside it have long sought to exploit domestic divisions like inequality and injustice. This is a global issue, demanding action from both advanced and emerging democracies.

The U.S., for example, could take a wider view of combating disinformation, featuring three parts.

First, more integration of disparate efforts is vital. That does not mean establishing an independent agency (as in Indonesia), for example, or focusing tenaciously on censorship and surveillance (as in India), but it could mean the current Federal Trade Commission and Justice Department investigations into tech giants including Facebook should include disinformation as one focus.

Second, social media firms—including Facebook—could agree to comply by the EU Code for Disinformation globally, as some are already doing with the EU's data privacy regulations.

Third, media literacy and education is imperative to help inoculate citizens against disinformation. Educational reforms are urgently needed to help students recognize disinformation when they see it, a topic all the more important given the rise of deepfakes.

In short, by working together and taking these threats seriously, we might even be able to find a way that—despite the challenges—democracy can persist even in a hyperconnected future.

This article is republished from The Conversation under a Creative Commons license. Read the