'Internet of things' could be an unseen threat to elections

6 March 2020, by Laura Denardis

Your home security systems knows when you leave for work, and when you get back. Credit: ESB Professional/Shutterstock.com

The app failure that led to a chaotic 2020 Iowa caucus was a reminder of how vulnerable the democratic process is to technological problems—even without any malicious outside intervention. Far more sophisticated foreign hacking continues to try to disrupt democracy, as a rare joint federal agency warning advised prior to Super Tuesday. Russia's attempt to interfere in the 2016 election has already revealed how this could happen: social media disinformation, email hacking and probing of voter registration systems.

The threats to the 2020 election may be even more insidious. As I explain in my new book, "The Internet in Everything: Freedom and Security in a World with No Off Switch," election interference may well come through the vast constellation of always-on, always-connected cameras, thermostats, alarm systems and other physical objects collectively known as the "internet of things."

The social and economic benefits of these devices are tremendous. But, in large part because the devices are not yet adequately secure, they also raise concerns for consumer safety, national security and privacy. And they create new vulnerabilities for democracy.

It is not necessary to hack into voting systems themselves but merely co-opt internet-connected objects to attack political information sites, stop people from voting, or exploit the intimate personal data these devices capture to manipulate voters.

Disrupting political communication

Connected objects have already been hijacked to shut down internet traffic.

The Mirai botnet of 2016 hijacked insecure video cameras and other home devices to launch a massive "distributed denial of service" attack that blocked access to many popular sites, including Reddit and Twitter. More recently, the FBI arrested a hacker for allegedly disrupting a California congressional candidate's website, flooding it with so many false requests it became inaccessible for legitimate views.

Similar political attacks that hijack some of the billions of often insecure connected devices could disrupt campaign websites and social media. They could also restrict public access to government websites with information about how and where to vote, as well as news reports on election results.

Preventing people from voting

Beyond blocking access to political information, a foreign agent or group might seek to stop people from voting by creating targeted chaos, whether by disrupting power systems, generating false weather or traffic reports, or otherwise triggering local emergencies that divert attention on Election Day.

Smart cities and the industrial internet of things are already targets, as evidenced by the yearslong history of Russia-attributed disruptions to Ukrainian power systems. Hacking home alarm or water systems could create politically micro-targeted local emergencies that distract people who would otherwise vote.

This type of local disruption in swing districts would be more likely to evade public or press scrutiny than an outright hack of election machines or vote-tallying systems.

Making phishing hacks more credible

The massive amount of intimate data these devices collect—when someone enters a building, drives a car, uses a sink, or turns on a coffee machine—could also make political operatives more susceptible to highly targeted spear phishing attacks. These tactics trick people into relinquishing personal information or clicking on malicious links—mistakes that gave hackers access to Democratic National Committee emails in 2016.

Similar phishing attempts on political campaigns continue, seeking to infiltrate email accounts used by presidential and down-ballot candidates. The more believable they are, the more effective they are – so an email referencing personal facts gleaned from connected objects would make these attacks more potent.

Not being surprised again

More things than people are now connected to the internet. These connected objects are a new terrain for election interference—and people shouldn't be surprised if they're used that way.

To address this over the long term, customers will have to demand better privacy and security from their connected devices, such as doorbells and lightbulbs. Companies—and political institutions—that connect these devices to their networks will have to build in appropriate safeguards. Manufacturers will also have to design better protections into their devices. There may also need to be data privacy laws limiting how personal information is collected and shared.

More immediately, though, it is essential not only for state and local authorities and intelligence communities to remain vigilant, but for citizens to take security precautions with their own devices, and be on high alert for personalized attempts to influence or disrupt their political participation.

Preserving democracy now requires taking seriously the consequences of the internet being deeply embedded in the physical world—the internet in everything. We are all responsible.

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

Provided by The Conversation

APA citation: 'Internet of things' could be an unseen threat to elections (2020, March 6) retrieved 2 July 2022 from https://techxplore.com/news/2020-03-internet-unseen-threat-elections.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.