Opinion: Technology, once thought the enabler of democracy, is threatening to kill it off

May 8 2017, by David Glance

French voter. Credit: Rama/Wikimedia, CC BY-SA

Democracy has entered a new phase marked by hacking by foreign states and fake stories shared on social media aimed at damaging political

parties.
The social media companies have so far been mostly incapable, or unwilling, to do anything about the fact that a large part of the dissemination of this "fake news" has been through automated software programs posting on Twitter.

The French presidential election didn't escape malicious "information operations" after the party of leading favourite, Emmanuel Macron, was hacked and nine gigabytes of emails, documents and photos posted on the internet Friday evening.

The French presidential election has had its share of "fake news" including a claim repeated by right wing National Front leader, Marine Le Pen, that opponent Emmanuel Macron has an offshore account in the Bahamas. This accusation appears to have originated on the notorious online bulletin board 4chan, but its lack of credibility didn't stop the right-wing leader from quoting it in an attempt to at least fuel the story for mainstream media and social media.

The strange part of the hacked emails release was the timing – just before the start of a media blackout period where presidential candidates are banned from communicating or reporting anything that could be construed as electoral propaganda. Since the documents contain emails up until April 24th 2017, the hackers would have been able to release them with presumably more effect well before this time.

The late release of the dump, combined with the media blackout, means its effect on the election is likely to be minimal. Wikileaks has already reported that metadata in the dump features Cyrillic writing and mentions the name of an employee of a Russian government security contractor Evrika, raising the possibility of Russian involvement.

At this time, however, it is really not possible to conclude very much about the authenticity of the data or who could have been behind its hack and release. Digital fingerprints, such as those found in the metadata of the dumped files, is hardly conclusive evidence of the identity of the perpetrators. The inclusion of Cyrillic metadata with names tied to the Russian Federal Security Services (FSB), could just as easily have been other nations' security services attempting to implicate and discredit Russia. In fact, this last possibility would explain the release of files at the last minute when it was very unlikely to have had much impact on the outcome of the election.

Whoever was responsible for the hack, the National Front and far-right activists in France and the United States quickly have tried to exploit the release on Twitter, making it briefly a trending topic.

There is a lesson however for all future elections and their political participants about how technology has come to dominate the political process.

First, social media, once believed to be the vehicle for true democratic expression by the public, has become a morass of disinformation, easily manipulated through software. Second, the production of fake news supported by falsified photos and documents has become another mainstream tactic employed by anyone and everyone wanting to influence electoral outcomes. Third, it is certain that political parties will be hacked and there is little they can do to prevent it happening.

Dealing with this new political reality is going to be difficult, but at least governments and political parties will not need much persuading that something needs to be done to stop the democratic process from being entirely subverted.

The first thing governments could do would be to force social media companies such as Facebook and Twitter to deal with automated "bots" that are responsible for amplifying the spread of disinformation. Technically, this would be easy for such platforms to do and it is unclear why they haven't done so already.

Preventing political party communications from being hacked is going to be an impossible task. Phishing emails are becoming increasingly sophisticated. A recent spate of phishing emails targeting Google Docs users is fooling even technically adept users. Employees of political parties will have to become much better at scrupulously deleting emails and documents that contain anything that would cause issues if they became public. Encryption should be used for documents that absolutely need to be kept secret.

On a more optimistic note, it seems fake news may be something that loses its potency with time. The fact this phenomenon is now widely understood means that disinformation is being identified and countered before it has much impact. The public is also getting better at discounting unreliable sources of information.

There is also the process of habituation. After a continuous succession of outlandish claims made on social media, people simply stop listening.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Opinion: Technology, once thought the enabler of democracy, is threatening to kill it off (2017, May 8) retrieved 23 April 2024 from https://phys.org/news/2017-05-opinion-technology-thought-enabler-democracy.html